

国际信息工程先进技术译丛

WILEY

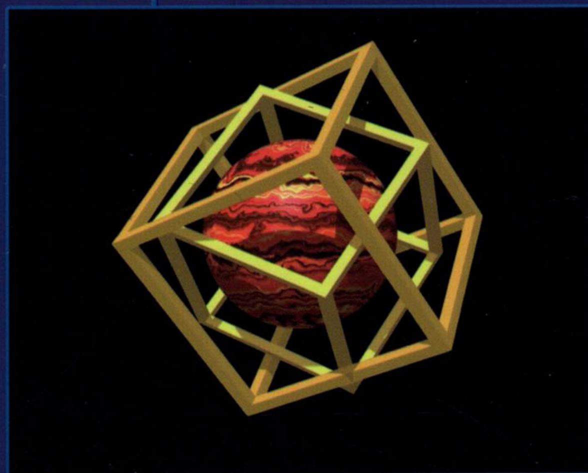
M2M通信

M2M Communications: A Systems Approach

David Boswarthick
（法） Omar Elloumi 著
Olivier Hersent
薛建彬 等译









机械工业出版社
CHINA MACHINE PRESS

VISIT…

LANZAROTE
Caliente.COM

本书特色

- 本书是第一部有关M2M技术及业务介绍的书籍，并从标准化的视角来讨论M2M相关技术。
- 涵盖了当前M2M行业主要面临的挑战，并提出了潜在的优化解决方案。
- 提出了M2M的系统级架构，并明确定义了系统的一些方法和接口。
- 为从事M2M和物联网领域的工程师们提供了许多重要信息。
- 提出了一个M2M水平领域和垂直领域交叉的概念，并给出了一个可能的演化路径。



国际信息工程先进技术译丛

M2M 通 信

David Boswarthick
（法） Omar Elloumi 著
Olivier Hersent
薛建彬 等译



机 械 工 业 出 版 社

近几年，物联网从诞生到迅速发展，受到了产业界及学术界的广泛重视，并上升到国家战略性新兴产业的高度。物联网的概念和内涵目前仍处于不断发展之中，物联网涉及的技术较多，其中 M2M 技术也是其核心技术之一。

本书紧跟 M2M 应用的最新发展，结合 M2M 工程应用的研究成果，采用通俗易懂的语言阐述相关技术，内容系统全面，材料充实丰富。在文字叙述中突出基本概念、基本理论及系统涉及的核心技术，同时对 M2M 的业务模式进行了探讨，重点讲述 M2M 系统的特点及相关技术的使用，书中还对 M2M 的架构及协议进行了详细的介绍，并对 M2M 技术的未来发展进行了展望。读者通过对各章节的学习将对构建 M2M 应用系统有一个较为全面的认识，从中学习到 M2M 技术核心理论，为 M2M 系统的实施及应用打下良好的基础。

本书适合物联网领域的研究人员和工程技术人员阅读，也可以作为物联网及相关专业的高年级本科生、研究生和教师的专业参考书。

Copyright © 2012 John Wiley & Sons Ltd

All Rights Reserved. This translation published under license. Authorized translation from the English language edition, M2M communications: a systems approach, 978-1-119-99475-6, by David Boswarthick, Omar Elloumi, Olivier Hersent, published by John Wiley & Sons, Ltd. No part of this book may be reproduced in any form without the written permission of the original copyrights holder.

本书中文简体字版由机械工业出版社出版，未经出版者书面允许，本书的任何部分不得以任何方式复制或抄袭。版权所有，翻印必究。

本书版权登记号：图字 01-2012-7586 号

图书在版编目（CIP）数据

M2M 通信/(法) 博斯沃西克（Boswarthick，D.）等著；薛建彬等译. —北京：机械工业出版社，2013.4（2016.7 重印）
（国际信息工程先进技术译丛）
书名原文：M2M communications：a systems approach
ISBN 978-7-111-41693-7

Ⅰ.①M… Ⅱ.①博…②薛… Ⅲ.①移动通信－研究 Ⅳ.①TN929.5

中国版本图书馆 CIP 数据核字（2013）第 039663 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策划编辑：牛新国 责任编辑：闾洪庆
版式设计：霍永明 责任校对：闫玥红
封面设计：马精明 责任印制：乔 宇
北京机工印刷厂印刷（三河市南杨庄国丰装订厂装订）
2016 年 7 月第 1 版第 2 次印刷
169mm×239mm · 18 印张 · 358 千字
标准书号：ISBN 978-7-111-41693-7
定价：68.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务	网络服务
服务咨询热线：010-88361066	机 工 官 网：www.cmpbook.com
读者购书热线：010-68326294	机 工 官 博：weibo.com/cmp1952
010-88379203	金 书 网：www.golden-book.com
封面无防伪标均为盗版	教育服务网：www.cmpedu.com

译 者 序

现代通信工具的发展促使我们的社会飞速前进。交流与沟通已经不仅仅局限于人类之间，科技的发展使得另外一种交流形式应运而生：机器对机器（Machine to Machine，M2M）通信。它是一种让机器“开口讲话”的技术，近年来已成为通信产业界的热门词汇。M2M技术具有广阔的市场和应用前景，它将会为整个通信产业带来极大的发展机遇和经济增长，同时还将会推动人们社会生产和生活方式新一轮的变革。

欧洲电信标准化协会（ETSI）M2M技术委员会目前正在发挥主导作用，推动M2M领域规范和标准化的制定工作。欧洲电信联盟M2M技术官员David Boswarthick在本书中全面地介绍了M2M的标准和系统架构的相关概念及具体实现，以及M2M技术未来的发展前景。作者提出把机器对机器的服务和主流的相关通信技术结合起来作为一个大的系统从整体上提供M2M的解决方案。书中阐述了在电信网络解决方案中目前正在实施的由ETSI（欧洲电信标准化协会）和3GPP（第三代合作伙伴计划）提出的最新通信标准，这为M2M技术的发展提供了产业化和标准化的支持。

作者在书中全面介绍了M2M的业务模式，M2M的架构及协议，M2M的应用，M2M业务架构，M2M通信方案，M2M网络优化及M2M安全性等各个方面的技术信息。作者还就M2M在智能仪表、智能电网和电子健康等主要应用领域的应用展开探讨。作为一门复杂技术领域的高级导论课程，通过本书的学习可以使读者能进一步掌握端对端技术的基础理论知识和基本技能。

本书具有以下几个特点：

1）本书是第一部有关M2M技术及业务介绍的书籍，并从标准化的视角来讨论M2M相关技术。

2）涵盖了当前M2M行业主要面临的挑战，并提出了潜在的优化解决方案。

3）提出了M2M的系统级架构，并明确定义了系统的一些方法和接口。

4）对从事M2M和物联网领域的工程师们提供了许多重要信息。

5）提出了一个M2M水平领域和垂直领域交叉的概念，并给出了一个可能的演化路径。

本书内容极其丰富，可以作为物联网工程及通信工程等相关专业学生学习M2M技术的教材和自学参考书，也适合信息类专业人士自修提高使用。

本书由薛建彬、马维俊、王志良组织翻译，秦立静、赵燕琴、梁波共同完成了

本书的翻译、录入、校对等工作。

译者在翻译过程中，对原书存在的一些错误进行了修正，以便进行正确的翻译。如果书中仍然存在疏忽与错误之处，恳请读者批评指正。

译 者

原　书　序

我非常荣幸地接受作者邀请为M2M和物联网两本系列书的第一本《M2M通信》撰写序言。

尽管机器对机器（M2M）的设备和应用市场仍然处于发展阶段，但我们已经可以预见，这项技术将对我们的生活产生深远的影响。随着对新应用领域的探索，我们可以对M2M市场的发展有许多预测。例如，据估计移动设备从目前的约60亿，最终将增加到超过500亿移动连接的机器。其他的估计表明，到2012年，M2M和物联网的市场产值将达到115亿美元。事实上，M2M市场可以按众多方式来划分，如根据硬件设备和软件来划分；根据连接技术或依照特定的行业应用领域来划分。

既然M2M所使用的许多技术已经存在了数年，为何M2M市场的发展到现在才突然发力？现今M2M发展的一个关键因素是无处不在的、低成本连接的普及。我们已经习惯于低价、高速的家庭和企业互联网接入。现在许多地区的第三代移动通信3G网络和未来的第四代移动通信LTE网络提供类似的接入速度，极具价格竞争力。忽然间，一个我们所梦想和需要的互联网网络连接的主机应用时代来临，它已经变得十分经济。

在家居和工业领域中，大规模部署基于IP连接的传感器、监视器和驱动器，使我们可以开发新的互连的、可互操作的服务，这将会改变我们的日常生活。M2M技术提供了在现实中采用混合技术搭建应用的视野，利用多个新信息来源，搭建虚拟世界web服务。这一设想被称为“物联网”，在物联网中连接的事物并不是最重要的，相反，最重要的是连接事物所提供的信息，以及人们如何将信息结合起来，呈现和使用这些信息，并在此基础上做出决策。物联网提供了一个新的技术视角，我们必须超前地看到它对社会的影响，以便于我们理解如何使用这种技术来使我们未来的生活变得更加美好。

展望未来，我们怎样才能建立一个灵活的M2M架构，其主要的特征需要我们将多样的技术、功能和需求考虑在内，并且此架构能很好地将现今及未来的各种技术融入其中？我们怎样才能提高互操作性？我们如何才能保护信息的保密性和隐私，而不是限制潜在有利的新应用？我们如何才能确保建立的这些系统的可靠性，因为我们越来越依赖于这些技术的发展？应对这些挑战的解决方案不在于任何一个组织或个人。这需要跨行业思维，它需要不同的有关行动者之间的合作，它需要在国际层面上的协调。达成一致共识的国际标准对确保M2M的技术和市场发展是必

不可少的，提供全面解决方案，其中存在许多挑战。欧洲电信标准化协会（ETSI）M2M 技术委员会目前正在发挥主导作用，推动这一领域的国际标准化工作。

除了面对广泛的社会挑战，我们还面临着许多复杂的技术问题。快速部署和采用 M2M 的技术将导致我们现有网络上叠加了新的需求。M2M 业务在网络方面，往往需要高效率、低开销、低功耗和更大的灵活性。这些需求将遭遇现有网络高速、低延迟和大容量需求的瓶颈。我们可能需要重新思考我们该如何设计以及如何管理我们的网络，如果 M2M 业务成为普遍预期，我们需要考虑新的接入技术，以使新的无线技术更好地服务于新的应用。

我们所确定的电信和数据网络标准将会对 M2M 应用的增长产生深远影响。欧洲电信标准化协会（ETSI）已经在这方面开展了多年的工作，来推动规范和标准的制定工作。我敢肯定，本书将对我们完成这项任务提供有益的指导，并帮助我们更好地理解和解决这些问题，以创建一个 M2M 的世界。

Luis Jorge Romero
欧洲电信标准化协会总干事

贡献者名单

Samia Benrachi-Maassam
Network & Services Architect
Bouygues Telecom
299 Ter Avenue Division Leclerc
92290 Chatenay-Malabry, France

David Boswarthick
Technical Officer, TC M2M
ETSI
650, Route des Lucioles
06921 Sophia Antipolis, France

Ioannis Broustis
Member of Technical Staff
Alcatel-Lucent
600 Mountain Avenue
Murray Hill, NJ 07974, USA

Emmanuel Darmois
Vice President, Standards
Alcatel-Lucent
7–9 Avenue Morane Sauliner, BP 57
78141 Velizy, France

Omar Elloumi
Director Standardisation, M2M and Smart Technologies
Alcatel-Lucent
7–9 Avenue Morane Sauliner, BP 57
78141 Velizy, France

François Ennesser
Technical Marketing – Standardization & Technology
Gemalto S.A.
6 rue de Verrerie
92190 Meudon, France

Claudio Forlivesi
Research Engineer
Alcatel-Lucent
Copernicuslaan 50
2018 Antwerp, Belgium

Bruno Landais
Network Architect
Alcatel-Lucent
4 rue L. de Broglie, BP 50444
22304 Lannion, France

Ana Minaburo
Independant Consultant
Cesson Sevigne Cedex, France

Simon Mizikovsky
Technical Manager
Alcatel-Lucent
600 Mountain Ave.
Murray Hill, NJ 07974, USA

Toon Norp
Senior Business Consultant
TNO
Brassersplein 2,
NL-2612 Delft, Netherlands

Franck Scholler
E2E Network Solution Architect Manager
Alcatel-Lucent
7–9 Avenue Morane Sauliner, BP 57
78141 Velizy, France

Ganesh Sundaram
Distinguished Member of Technical Staff
Alcatel-Lucent
600 Mountain Ave.
Murray Hill, NJ 07974, USA

Laurent Toutain
Associate Professor
Telecom Bretagne
2 rue de la Chataigneraie, CS 17607
35576 Cesson Sevigne Cedex, France

Harish Viswanathan
CTO Advisor
Alcatel-Lucent
600 Mountain Ave.
Murray Hill, NJ 07974, USA

Gustav Vos
Director, Technology Standards
Sierra Wireless
13811 Wireless Way
Richmond, BC, V6V3A4, Canada

目　　录

译者序

原书序

贡献者名单

第1章　M2M简介 …… 1
1.1　什么是M2M …… 2
1.2　M2M的业务模式 …… 5
1.3　促进M2M技术的成熟 …… 9
1.3.1　M2M高层框架 …… 9
1.3.2　政策和政府的鼓励措施 …… 10
1.4　M2M标准 …… 12
1.4.1　选择哪一个标准 …… 12
1.5　本书路线图 …… 17
参考文献 …… 18

第1部分　M2M现今发展状况

第2章　M2M的业务模式 …… 20
2.1　M2M市场 …… 20
2.1.1　医疗保健行业 …… 21
2.1.2　物流行业 …… 21
2.1.3　能源行业 …… 22
2.2　M2M市场的接受：驱动及障碍 …… 23
2.3　M2M价值链 …… 25
2.4　市场规模预测 …… 26
2.5　商业模式 …… 27
2.5.1　网络运营商或CSP主导模式 …… 28
2.5.2　MVNO主导模式 …… 29
2.5.3　企业客户主导模式 …… 30
2.6　M2M业务指标 …… 30
2.7　市场演变 …… 31

参考文献 …… 32

第3章　早期M2M部署的经验教训 …… 33
3.1　引言 …… 33
3.2　早期M2M运营部署 …… 33
3.2.1　引言 …… 33
3.2.2　早期M2M运营部署举例 …… 35
3.2.3　早期M2M部署常见问题 …… 42
3.2.4　M2M部署可能的优化 …… 44
3.3　本章小结 …… 47
参考文献 …… 47

第2部分　M2M的架构及协议

第4章　M2M的需求及高层架构原则 …… 50
4.1　引言 …… 50
4.2　用例驱动的方法实现M2M需求 …… 50
4.2.1　何谓用例 …… 50
4.2.2　ETSI M2M的用例 …… 51
4.2.3　用例开发的方法论 …… 51
4.3　ETSI M2M智能计量方法 …… 52
4.3.1　引言 …… 52
4.3.2　典型的智能计量部署方案 …… 54
4.4　ETSI M2M中的电子健康方法 …… 57
4.4.1　引言 …… 57
4.5　ETSI M2M服务要求：高层概括和不同细分市场的适用性 …… 61
4.6　M2M中流量模型及特殊方法对网络架构设计的要求和思考 …… 63
4.6.1　为何使用无线网络 …… 63
4.7　M2M细分市场/应用说明 …… 64
4.7.1　汽车 …… 64
4.7.2　智能遥测 …… 65
4.7.3　监控和安全 …… 66
4.7.4　销售点（PoS） …… 66
4.7.5　自动售货机 …… 66
4.7.6　电子健康 …… 67
4.7.7　视频直播 …… 67
4.7.8　楼宇自动化 …… 68

4.7.9 M2M 工业自动化 …… 68
4.8 M2M 交通解决方案 …… 68
4.8.1 智能计量通信特性 …… 69
4.8.2 全局业务特性 …… 72
4.9 M2M 通信的高层架构原则 …… 78
4.10 本章小结 …… 80
参考文献 …… 81

第5章 ETSI M2M 业务架构 …… 82
5.1 引言 …… 82
5.2 高层系统架构 …… 84
5.3 ETSI TC M2M 服务功能框架 …… 87
5.4 ETSI TC M2M 的版本1方案 …… 89
5.5 ETSI M2M 的服务功能 …… 90
5.5.1 可达性、寻址能力、知识库性能（xRAR） …… 90
5.5.2 远程实体管理性能（xREM） …… 91
5.5.3 安全性能（xSEC） …… 94
5.6 M2M 的 REST 架构格式简介 …… 95
5.6.1 REST 简介 …… 95
5.6.2 为何在 M2M 中使用 REST …… 96
5.6.3 REST 基础 …… 98
5.6.4 在 M2M 中应用 REST …… 99
5.6.5 附加功能 …… 100
5.7 ETSI TC M2M 基于资源的 M2M 通信及规程 …… 109
5.7.1 引言 …… 109
5.7.2 在本节中使用的定义 …… 111
5.7.3 资源结构 …… 111
5.7.4 接口程序 …… 115
5.8 本章小结 …… 122
参考文献 …… 123

第6章 公共移动网络中的 M2M 优化 …… 124
6.1 概述 …… 124
6.2 基于通信网络的 M2M …… 124
6.2.1 引言 …… 124
6.2.2 M2M 通信方案 …… 125
6.2.3 移动或固定网络 …… 127

6.2.4　M2M应用的数据连接 …… 129
6.3　M2M的网络优化 …… 132
6.3.1　引言 …… 132
6.3.2　3GPP机器类通信网络改进的标准化 …… 132
6.3.3　降低成本 …… 133
6.3.4　M2M的增值服务 …… 140
6.3.5　编号、标识及寻址 …… 146
6.3.6　触发优化 …… 152
6.3.7　过载和拥塞控制 …… 158
参考文献 …… 167

第7章　IP在M2M中的作用 …… 168
7.1　引言 …… 168
7.1.1　IPv6简介 …… 169
7.1.2　邻居发现协议 …… 171
7.2　M2M中的IPv6 …… 172
7.3　6LoWPAN …… 173
7.3.1　框架 …… 174
7.3.2　头信息压缩 …… 174
7.3.3　邻居发现 …… 179
7.4　低功耗有损网络路由协议（RPL） …… 182
7.4.1　RPL网络拓扑 …… 184
7.5　CoRE …… 187
7.5.1　消息格式 …… 188
7.5.2　传输协议 …… 190
7.5.3　REST架构 …… 193
参考文献 …… 196

第8章　M2M的安全性 …… 197
8.1　引言 …… 197
8.1.1　蜂窝M2M的安全特性 …… 198
8.2　M2M生态系统中的委托关系 …… 201
8.3　安全要求 …… 206
8.3.1　客户/M2M设备用户 …… 206
8.3.2　接入网络提供商 …… 207
8.3.3　M2M服务提供商 …… 207
8.3.4　M2M应用提供商 …… 207

8.3.5 需求引导 …… 208
8.4 哪些类型的解决方案是合适的 …… 209
8.4.1 阻止黑客行为的途径 …… 209
8.4.2 公钥解决方案 …… 210
8.4.3 基于智能卡的解决方案 …… 213
8.4.4 基于预分配的对称密钥的方法 …… 214
8.4.5 基于身份加密的自引导协议 …… 215
8.4.6 M2M 设备组的安全性 …… 218
8.5 安全 M2M 和 MTC 通信的标准化工作 …… 220
8.5.1 ETSI M2M 安全性 …… 220
8.5.2 3GPP 安全性相关的机器类通信网络性能提升 …… 221
参考文献 …… 222

第 9 章 M2M 终端和模块 …… 224
9.1 M2M 模块分类 …… 224
9.1.1 接入技术 …… 224
9.1.2 物理形式因素 …… 227
9.2 硬件接口 …… 230
9.2.1 电源接口 …… 230
9.2.2 通用串行总线（USB）接口 …… 230
9.2.3 通用异步接收器/发送器（UART）接口 …… 231
9.2.4 天线接口 …… 231
9.2.5 通用集成电路卡（UICC）接口 …… 231
9.2.6 通用输入输出（GPIO）接口 …… 232
9.2.7 串行外围接口（SPI） …… 232
9.2.8 I^2C 接口 …… 232
9.2.9 模-数转换器（ADC）接口 …… 232
9.2.10 脉码调制（PCM）接口 …… 232
9.2.11 脉宽调制（PWM）接口 …… 232
9.2.12 模拟音频接口 …… 232
9.3 温度和耐久性 …… 232
9.4 服务 …… 233
9.4.1 应用执行环境 …… 233
9.4.2 连接性服务 …… 234
9.4.3 管理服务 …… 235
9.4.4 应用服务 …… 237
9.5 软件接口 …… 237

9.5.1　AT 指令 …… 238
9.5.2　软件开发工具包（SDK）接口 …… 238
9.6　蜂窝认证 …… 239
9.6.1　电信产业认证 …… 239
9.6.2　移动网络运营商（MNO）认证 …… 240

第 10 章　M2M 通信中的智能卡 …… 241
10.1　引言 …… 241
10.2　M2M 通信的安全性及隐私问题 …… 241
10.3　采用基于硬件的安全解决方案的理由 …… 242
10.4　独立安全要素及可信环境 …… 244
10.4.1　M2M 设备可信的环境 …… 244
10.4.2　可信未知设备：需要安全认证 …… 245
10.4.3　智能卡模型的优点 …… 246
10.5　M2M 环境下特定智能卡属性 …… 248
10.5.1　可移动智能卡与嵌入式安全要素 …… 248
10.5.2　UICC 抗环境制约 …… 251
10.5.3　用于无人值守设备的自适应卡应用工具包 …… 253
10.5.4　使用工具包命令到达 UICC 外围设备 …… 254
10.5.5　第三方应用的安全及远程管理 …… 255
10.6　智能卡在 M2M 环境中的未来演变 …… 256
10.6.1　基于集成电路的 M2M 服务标识模块应用 …… 256
10.6.2　UICC 的互联网协议集成 …… 256
10.7　M2M 的安全要素的远程管理 …… 257
10.7.1　综述 …… 257
10.7.2　后期个性化订阅 …… 257
10.7.3　现场远程管理订阅 …… 258
参考文献 …… 259

第 3 部分　本书结语及对未来的展望

第 11 章　结语 …… 262
附录　缩略语 …… 264

第 1 章　M2M 简介

Emmanuel Darmois，Omar Elloumi
阿尔卡特朗讯公司，维利兹，法国

M2M（Machine-to-Machine，机器对机器）已经走向成熟。从扩大连接“网络”（无线、有线；私有部门、公共部门）实体范围的想法开始，而不仅仅是人类和他们的首选通信设备出现在“物联网”（IoT）、“互联网对象”或 M2M 的概念中，这已经有将近十年了。最初的想法是，无数很大程度上不被人类注意到的新设备共同作用去扩大终端用户服务的足迹。这将创造一种新的方式来考虑安全性或舒适性，优化各种货物传送的机制，确保人或车辆追踪的有效性，同时创造出新的系统，产生新的价值。

每一个愿望都需要花时间来实现。早期的努力主要集中在通过测试新的商业模式，发展关键点的解决办法来测试可行性，并预测互操作性不足的影响来提炼最初的想法。在过去的几年中，人们意识到能够出现一种新的满足可行性需求的资源并且能货币化，这种想法通过行业的推动将东拼西凑的独立元素和解决方案变成一个连贯的“系统的系统”，逐步把重点从“什么”转向“如何”，并开发适合的技术和标准。

本章主要介绍 M2M 概念，并从今天众多可用的定义中提出了一个定义。它概述了新兴 M2M 业务的主要特点，提出了一种 M2M 框架的高级视图，这种框架将在随后的章节中进一步分解和剖析。另外，本章还分析了一些近些年出现的很大程度上使 M2M 开发成为可能的主要变化，也就是作为市场塑造者出现的规则和标准。这个标准是本书的中心主题之一，通过这个复杂的生态系统为主要的参与者和最近相关工作的状态提供指导。

最后，向读者介绍一下本套书的结构和内容，本套书实际上有两本。在读者手中不管是纸张的形式或是通过 M2M 应用程序下载到电子书阅读器上的形式，第一本书《M2M 通信》实质上介绍了 M2M 的框架需求，一些它主要系统方面的高级架构，例如 M2M 网络优化、安全和 IP 的角色。

第二本书《物联网：关键应用和协议》将讨论更多特定的“互联网对象”扮演角色的领域，也就是 M2M 网络领域，特别是相关的协议和这样网络的互联。从这个角度我们也能分析出一些未来 M2M 的应用，例如智能电网和家庭自动化。

1.1 什么是 M2M

许多人都试图对 M2M 这个缩略词提出一个单独的定义：机器对机器，机器对移动（反之亦然），机器对人，等等。本书中，M2M 被认为是机器对机器。定义完整的 M2M 概念不是一个简单的任务，这是由 M2M 的范围自然灵活，且范围也总是定义不清楚决定的。

也许描述 M2M 最基本的方式如图 1-1（M2M 的“本质”）所示。M2M 角色建立的条件是允许一个设备通过一个通信网络与业务应用程序交换信息，以便这个设备和/或应用程序能够作为信息交换的基础。在这个定义中，通信网络有一个关键角色：一个匹配的应用程序和设备很难被认为拥有 M2M 关系。这就是为什么 M2M 常常被缩短成 M2M 通信的缩略词，而它本身是 M2（CN2）M：机器对（通信网络对）机器的缩略词。

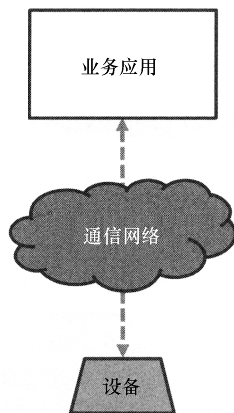


图 1-1 M2M 的本质

就其本身而言，这种描述仍然没有完全描述出 M2M 的特点。举个例子，一个移动电话在与一个呼叫中心应用程序交互的过程中并没有被看做是 M2M 应用程序，因为人起主导作用。为了澄清这一点，许多 M2M 关系中更复杂的特点在这种关系下被讨论。

在许多情况下，M2M 是一组相似的设备与一个单独的应用程序之间的相互作用，如图 1-2 所示。车队管理就是这样一个应用的例子，其中的设备例如卡车，而通信网络是一个移动网络。在某些情况下，如图 1-3 所示，因为能力有限，组中的设备也许不会直接与应用程序交互。在这种情况下，两者之间的关系是由另外一种能够整合通信形式的设备（例如，一个网关）调节的。“智能计量”是这样应用下的一个例子，其中的设备是智能电表，而通信网络可以是移动网络或是公共网络。

考虑到这一点，“M2M 区域网络”这个术语被欧洲电信标准化协会（ETSI）介绍出来。一个 M2M 区域网络提供了连接到同一 M2M 区域网络的不同 M2M 设备之间的物理层和 MAC 层的连通性，这样通过一个路由器或是网关就可以允许 M2M 设备来接入公共网络。

M2M 独特的特点主要是由于终端设备的关键角色决定。这些设备在信息与通信技术（ICT）领域并不是新的，但是，市场将会看到一个带有非常独特特点的 M2M 设备的新集合。这些特点将会在下面进一步讨论，特别是它们对那些直到现在还没有被认真考虑过的应用和网络需求的影响。

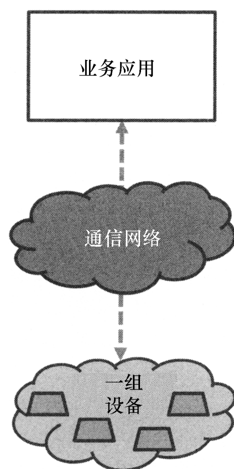


图 1-2　M2M 关系中的设备组

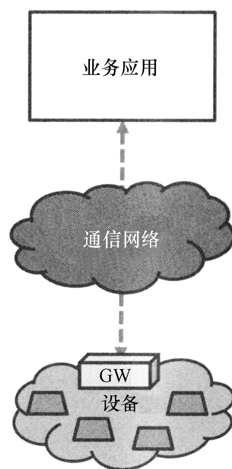


图 1-3　媒介化的 M2M 关系

- 多数性：这是 M2M 带来的最该被提倡的变化。人们普遍认为连接在 M2M 关系中的设备的数量在不久会大大超过那些与人类直接交互的设备的总和（例如，移动电话、个人电脑、平板电脑等)。这些设备的数量在一个数量级上的增加将导致更多应用程序结构上的压力，对于网络负载也是一样，将会在被设计用来容纳更少“角色”，更高级别和更多类型业务的系统上产生特定的可扩展的问题。这类问题的一个早期例子是 M2M 设备对移动网络的影响，而移动网络在设计思想中并没有为这些设备设计，在这个过程中系统要适应去允许大量设备带有非标准使用模式（这将在本章后面讨论)。
- 多样性：这里已经记录下了大量可能的应用到不同环境和业务领域的 M2M 用例。由于数据交换率、形式因素、计算和通信能力，最初 M2M 应用程序的实现已经导致了大量有多种需求的设备的出现。这种广泛多样性产生的一个结果就是异构性，对于互操作性，它本身就是一个巨大的挑战。这可能是普及 M2M 的一个主要障碍。为了定义和开发一般可能的能力，这对必须要在其上建立 M2M 应用程序的框架来说同样是个挑战。
- 不可见性：在许多 M2M 应用程序中有一个强烈的需求——这些设备常规传送它们的服务时必须用很少或不用人的控制。特别地，这就阻止了人类纠正错误（也防止了创造新的错误)。结果，设备管理与以往相比成为了服务和网络管理的关键部分，它需要被无缝地集成。
- 临界性：一些设备是生命保障者，例如在电子健康领域（血液采集器、压降探测器等)。许多是性命攸关的基础设施的关键元素，例如智能电网上的电压或相位侦测器、断路器等。这些用途在延迟和可靠性上有严格的要求，这将挑战和超过

现代网络的能力。

● 干扰性：许多新的 M2M 设备设计的意图很明确，那就是用来更好地管理一些系统，保证终端的良好、健康等。例子是已经提到的电子健康设备，用来测量的智能电表和/或家里用来控制电力消耗的设备等。这反过来会导致隐私的问题。实质上这对 ICT 系统不是一个新问题，但是这很可能会成为发展 M2M 系统的主要障碍。当大型智能电表的部署需要在终端用户的隐私权和能源经销商为了更好地符合日常能量消耗的需求之间做出优先权衡时，这可能会出现。

除了以上所列出的在 M2M 系统结构上的特点和影响，重要的是要考虑到 M2M 设备的其他一些特征，而这些设备在通过网络通信的方式上有额外的限制。这可能需要一种新的方式将这些设备聚在一起（图 1-3 中提到的媒介化的方法）。除此之外，设备可以是：

● 功能被限制的。大多数的 M2M 设备在计算能力上要比目前出现的现代笔记本电脑或智能手机低几个数量级。特别地，这些设备可能缺少远程软件更新能力。选择这种设计的一个主要原因是成本，这常常因为商业模式是需要非常有价格竞争力的设备（例如，许多情况下的智能电表）。功能的限制也是由理性的决定引起的，而这些决定是根据交换信息和可执行作用的属性做出的：最多的传感器并不意味着是活跃的、操作复杂的。

● 低功率的。虽然许多 M2M 设备与电力网相连，但是由于一系列的原因它们中的许多还需要不同的电力（常常是电池）。例如，它们中的大多数位于室外，它们不能轻易地与电源相连（例如，工业过程中的传感器、水表、路边监控）。这将减少这些设备与 M2M 应用程序之间交互的次数（例如，在信息交换的频率和质量方面）。

● 嵌入式的。许多设备将会在特殊的（敌对的，安全的）操作条件下部署在系统中，如果对系统自身没有重大的影响，这将很难去改变。例如，建筑或者车上的嵌入式系统很难去被替代（例如，当它们被焊接在汽车发动机上，而这些通常都是一些 M2M 设备）。

● 保持不变的。最后但是并非最不重要的是，许多新的 M2M 设备将会根据不同的期望寿命部署在非 ICT 的应用中。在许多有潜力的 M2M 业务领域，设备的更换率也许会比 ICT 工业的低。由于不同的业务模式（例如，没有运营商的设备补给），由于它们是嵌入式的这个事实，而且由于在设备运行的工业过程中演变的复杂性（例如，服务的关键性使得电力系统设备的更换很困难，这导致这个领域中设备很长的生命周期），这可能都会与成本问题联系起来。

关于 M2M 范围和定义清晰界限困难性的两点最后说明。

首先，由于在一些情况下，设备能够在常规和 M2M 两种模式下运行，所以常规 ICT 应用程序和 M2M 应用程序的分离就很大程度上纯粹是武断的。一个经典的

例子就是亚马逊的电子阅读器。尽管它是一种集中了人机功能（能使用电子书）和界面（电子书阅读器）的常规 ICT 设备，但它也是一种扮演终端用户电子书提供者角色的 M2M 设备。当终端用户决定买电子书，点击得到它时，电子阅读器设备通过一个服务器（用合适的格式提供一个合适的文件）和网络（常规移动网络）进入 M2M 模式。由于一系列促成因素，包括设备中的 SIM 卡、通过网络的设备安全鉴别、运营网络中设备的提前开通，这对终端用户是完全透明的。

第二，概述一些 M2M 设备与在所谓的物联网（IoT）中涉及的作为事物或对象设备之间的不同点是重要的。实际上，M2M 和物联网大部分是重叠的，但是一个并不是另一个的子集，它们各自还是有自己特别特殊的地方。

- 物联网是处理事物或是对象的，而 ICT 系统中 M2M 的关系可能不是这样。一个例子就是超市中向顾客提供带有射频识别（RFID）标签的物品。这些物品是被动的，没有直接的方法与 M2M 应用程序逆向地交流，但是它们能被 M2M 扫描仪所识别，这些扫描仪能够合计账单金额，同样为顾客做出另外的购买建议。从这个角度看，M2M 扫描仪是 M2M 关系的终结点。
- 这些设备之间最初的 M2M 关系是它们被看作是一个人与机器界面之间直接的扩展（例如，上面提到的电子阅读器终端），而不是作为物体（例如，终端用户冰箱）。

从长远看，一方面是在传统形式与 M2M 通信形式之间，另一方面是在物联网与 M2M 领域之间，相对人工的区别将会被 M2M 的发展和现有系统中整合更多物体的能力进一步模糊。

1.2　M2M 的业务模式

经过十年逐渐的发展，尽管许多属于雏形、早期的实现和商业的部署，但是已经有了大量记录下来的 M2M 用例，而它们中的一些在过去图样的基础上从没有进步。由于产生的收入和实体的生态系统，只有很少数创造出了有意义的业务模型。但是这种情况正在迅速地发展。

图 1-4 是 Beecham Research 关于 M2M 业务潜力的示意图，而 M2M 业务描述了 M2M 应用的主要部分。从这个角度出发，M2M 的潜在影响也被认为是很重要的，充分了解目前 M2M 的地位、阻止它快速出现的因素、加速它出现的措施是很必要的。这将在本书第一部分详细地解决。

图 1-4 中另一个有意思的方面是它从数据率和移动性两个主要观点把业务领域和相关设备联系了起来。前者作为 M2M 设备多样性的一个方面已经被解决。后者因为在许多目前已经出现的 M2M 应用程序中的关键性，它也是很重要的，例如智能计量。图 1-4 中，特别是设备移动性的指示表明相比移动设备会涉及更多潜在的

固定设备。可是，在 M2M 发展的现阶段，相对于基于有线网络的方法，基于已经被研究和部署的无线网络与蜂窝网络的方法是主要的。一个原因是它们从一些蜂窝网络可能的方面中受益。例如，部署作为移动设备的 M2M 设备的可能性（例如在设备中嵌入一个 SIM 卡），在工业设置中置入验证、安全和易配置。大量蜂窝网络中 M2M 应用程序的部署明显地驱动了这种需要来为固定的或是移动性低的 M2M 设备优化网络，用这种方法来减少整个连通性的成本。

不是为了试图建立整个 M2M 领域的名单和提供应用的例子，本节对于每一个主要 M2M 业务成熟性的调查是为了鉴定它涌现过程中的障碍和可能的促进因素。

图 1-5 提出了对成熟 M2M 工业阶段性的观点。用长远的眼光（20 年）描述了 M2M 部署的三个阶段。

目前 M2M 的关键阶段是蜂窝网络中心，在那里大多数的应用程序在遥测和快速管理的区域。它们大多使用现存的蜂窝网络基础设施，主要的企业对企业（B2B）应用程序的路由也是一样。考虑到我们快要到这个阶段的末尾，为了进入下一阶段（过渡），明确我们是否遇到这些条件就是很重要的，在下一阶段，很大比例的 M2M 市场将会被开发，特别是企业对消费者（B2C）应用程序，它将会比以前的 B2B 应用程序更被需要。

除了 M2M 技术的发展，仍然有很多挑战，最有压力的一些是：

- 解决方案的分离。在大量的例子中，迄今为止开发出的和实施的解决办法已经独立地解决了特定垂直应用程序的需求问题。这就根据技术、平台、数据模式的异构性创造了筒仓式的解决办法。互操作性一般是很受限制的或是不存在的。克服这个挑战至少需要两方面的努力。第一，必须定义更广泛的标准，特别是关于数据模型。另外，要有能够使多种应用程序重复使用的服务平台，避免由于一般能力的缺乏而对每一种应用程序完全重新设计的需要。
- 网络失调。如上所述，通信网络被设计用来满足许多实质上与 M2M 不同的需求，一个例子是没有设计去考虑大量设备的移动网络，这些设备产生很小数量的数据传输，以及潜在的大量控制超负荷和连接性平台（更不要说固定设备不需要漫游能力）。需要做许多对 M2M 业务的优化，这些必须在标准化下被替换。另一个例子是延迟，在一些应用中（例如，智能电网）延迟的需求是大大的低于 10ms，远程保护级别要比互联网协议语音（VoIP）级别低不止一级。
- 安全。正如已经概述的，一些最有前途的 M2M 应用（电子健康，智能电网）是安全至上的，它必须被做得强健来对抗多种安全威胁。这就要求这种安全需要通过标准和证明被精确地理解和开发。
- 隐私。为了开发和解决隐私这个敏感的问题，需要规则（一个必要的先决条件）和标准化。
- 服务能力。为了应对破碎的市场，必须通过几个应用程序概述重复使用的能

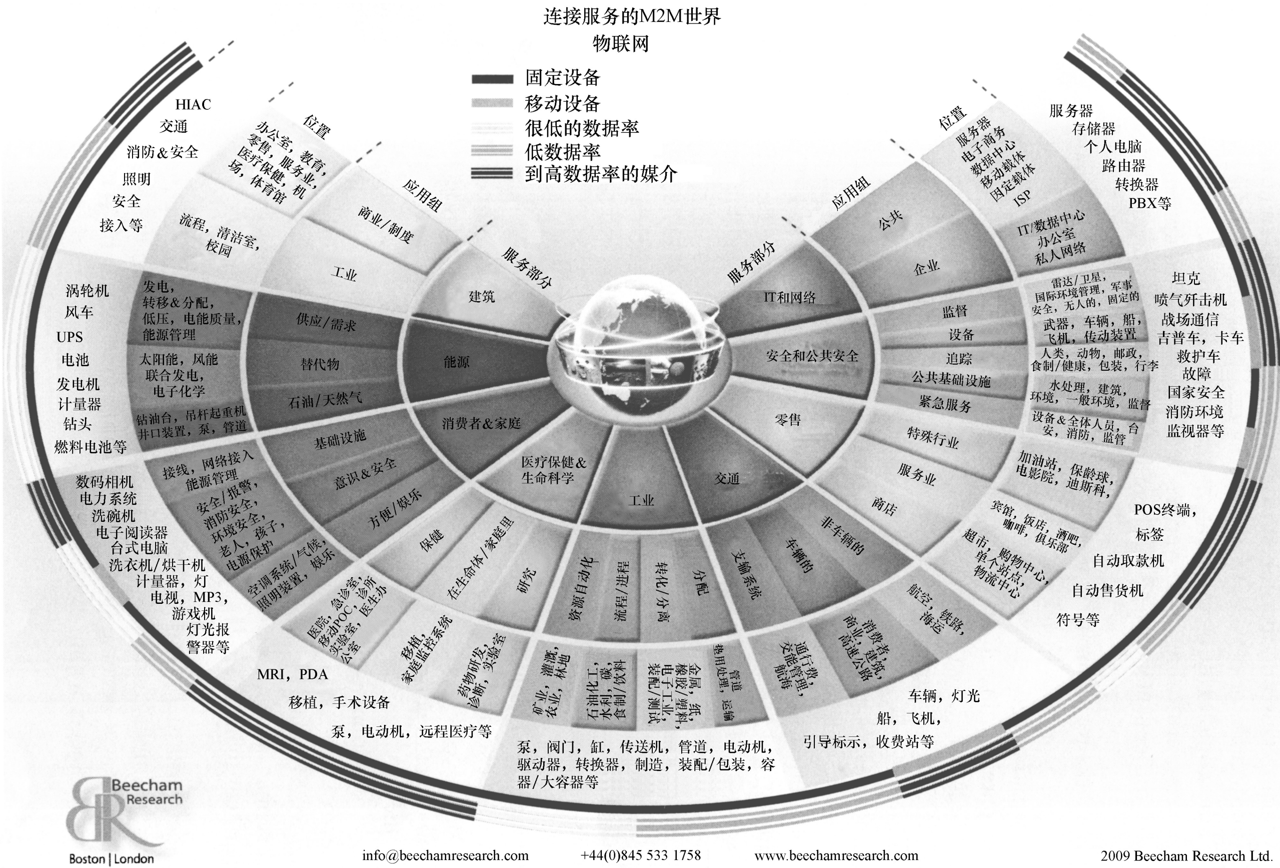


图1-4 M2M服务与设备（本图得到Beecham Research允许复制，还有作者提供的关于设备移动性和数据率的指示）

力。ICT 网络的历史表明这仍旧需要在不同的构架层之间做出一些分离。特别地，把应用程序从服务能力（例如，设备管理）和网络能力（例如，规则）中分离出来是关键。

● 测试，证明。大量的 M2M 解决方案将不得不在传统筒仓式服务之外开发，用其他 M2M 或是传统应用程序去整合。这需要很大程度上的互操作性和提供商的承诺，这将反过来使设备与装置的测试和验证组织成为必需。这成为工业和/或标准化组织或论坛的角色。

考虑了以上挑战，图 1-5 同样概述了三个主要的加速 M2M 成熟的因素，也就是：

● 高水平的框架。这指的是一套新兴的基于结构、平台、技术的标准，这是以允许开发非筒仓式的、不过时应用程序为方法整合的。特别地，这些框架允许规模经济，这将改变 M2M 业务模式的动态。

● 政策和政府鼓励措施。许多 M2M 挑战也许不会被工业独立的处理，根据这种意识，公共机构和政府已经开始在通过雄心激励计划刺激投资和政策制定中扮演积极的角色。这反过来驱动了在更宽广的 M2M 生态系统上的更多投资，同样创造了更多对 M2M 工业可行性的信任。

● 标准。来自各个行业（不仅是 ICT）的大量可靠的产业伙伴，大的或是小的，都已经开始一起工作，要创造出新的标准需求在全球系统的水平上处理 M2M。

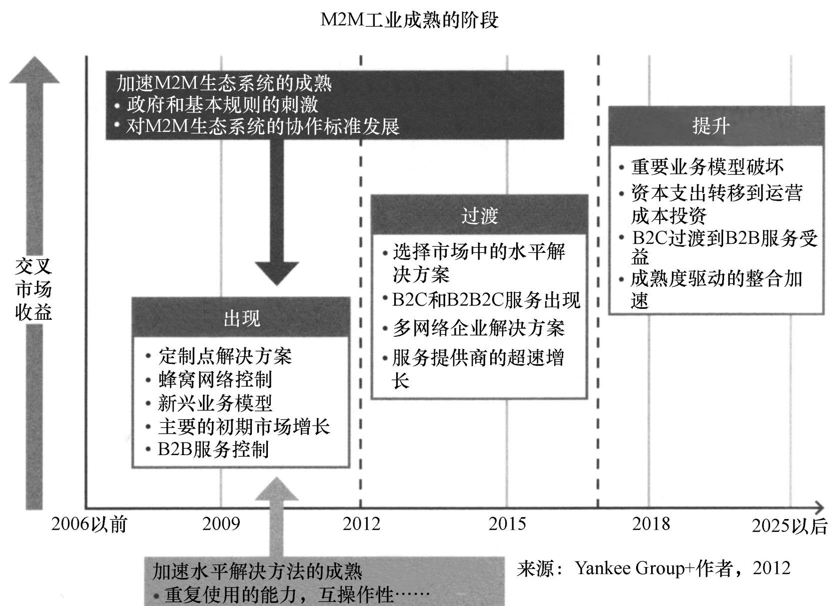


图 1-5　M2M 工业成熟的阶段（被 Yankee Group 允许复制）

本章和本书更多的地方将聚焦这些方面，特别是标准，用长远的眼光看，这些加速因素已经被利用，开始改变 M2M 的格局。

1.3　促进 M2M 技术的成熟

1.3.1　M2M 高层框架

M2M 角色面对的最大部分挑战是把垂直筒仓式转变成一套简单可发展的和递增可开展的应用程序。图 1-5 表明向 M2M 成熟性第二阶段过渡的标志是水平平台的出现和部署。

“水平”所表示的意思是一个贯穿业务领域、网络和设备，连贯的有效框架。这是一系列能够功能分离的技术、体系结构和过程，特别是应用层和网络层，如图 1-6 所示。

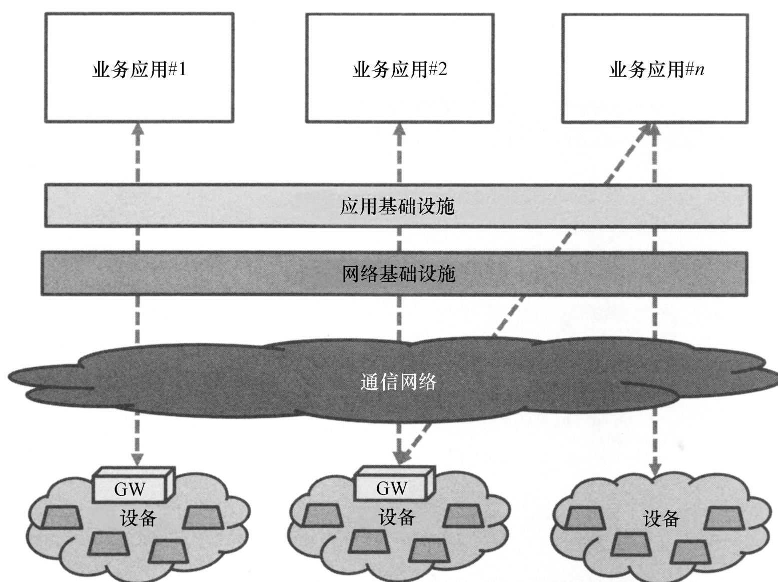


图 1-6　一个 M2M 的挑战：M2M 服务层的出现

这样一个平台将依靠一系列以软件模块为形式的功能，向 M2M 应用提供软件模块是为了促进它的发展、测试和部署的生命周期。通过彻底地分析行业内几个 M2M 应用用例及它们相关的需要得到它们确切的需求、可能性和定义公共服务的能力。

M2M 应用程序的开发和部署能够受益于一系列仔细的设计、测试和优化的构建模块，而不考虑部署的 M2M 应用的类型。本书剩余部分中，这种构建模块将作

为 M2M 服务能力被提到。

除了应用程序所用其他方面中的 M2M 服务能力，简单列举几个，比如，设备激活、设备监控、设备定位、数据存储、对水平平台（M2M 设备运行能力）的媒介化，这个概念的进一步发展使得 M2M 应用主要集中到了业务逻辑上。

一旦一系列固定的 M2M 服务能力被规定，合乎逻辑的下一步就是通过应用程序编程接口（API）的使用向 M2M 应用去揭示它们。这将是解决以下部分的标准。

1.3.2 政策和政府的鼓励措施

经过最初缓慢的进展，公共机构和政府现在已经意识到他们要在 M2M 通信的腾飞中扮演关键角色，特别是因为 M2M 在许多对他们国家或地区的将来确实必要的新系统中是一个完整的单元。已经得到了一些经验，在相关的鼓励措施定义中应用了一些方法，特别是让基础设施能够优化的标准，经济规模和服务能力可重用性的积极影响，去作为一个主流部署的主要促成者。由于以下原因，目前，大量政策和政府鼓励措施已经落实到位，去扮演一个重要，有时是相当关键的角色。

- 经济鼓励措施提供了一个有吸引力的、稳定的框架，在新项目和运行部署中为投资创造额外的机会。最著名的一个例子是美国复苏与再投资法案（ARRA）被奥巴马总统在 2009 年签署成为法律，他为能源效率、可再生能源的研究，以及以贷款担保为形式的投资、研发资助、工人的训练等拨出了超过 270 亿美元。
- 规则为一套可适用的，在一个国家或地区强制实行的标准的发展提供了明确的方向。例子包括欧盟委员会为智能计量［M/441］和应用射频识别和系统的 ICT 授权。另一个著名的例子是 2007 年的美国能源独立和安全法案（EISA），该法案向美国国家标准与技术研究院（NIST）分配了“主要的责任去协调一个框架的发展，这个框架包括为信息管理制定草案和模型标准，用它去实现智能电网和系统的互操作性……”［EISA］。
- 合作研究和项目发展的基金既是导致标准发展的一步，也是开发概念验证、验证现存标准的方法。一个重要的例子是欧盟的第 8 个框架计划［FP8］。

1.3.2.1 规则对 M2M 市场和标准的影响

一旦规则授权新的服务，紧接着是授权 M2M 结构的使用（例如，在全球系统中实现某种遵从度）或是 M2M 技术和设备的使用，它在 M2M 市场的增长中扮演了一个重要的角色。在世界各个地方这都是真的，欧洲可以被作为一个授权 M2M 技术规则取得进步的例子。

一个主要的例子是气候变化。欧盟已经通过提出“20-20-20”目标为电力部门通过了一个新的规则，作为欧盟成员国全球性的目标，这个目标是到 2020 年排放物减少 20%，可再生能源占 20%，能源效率提高 20%。作为这个目标的一部分，智能计量通过了各个欧盟成员国的授权。例如，法国已经正式通过了一个法

律，要求从 2012 年开始每一所新房子都要装备智能电表。

另一个值得注意的例子是网络电话，欧盟委员会的这个项目打算为在欧盟任何地方卷入冲突的司机带来快速的帮助。目标是在车辆上部署“黑匣子”蜂窝设备，就像 GPS 为当地紧急机构协调一样，它将发送事故的信息（根据安全气囊部署和传感器信息的影响）。除了早期不同汽车生产商的实施，比如，宝马汽车公司、法国标致/雪铁龙集团、沃尔沃集团，欧盟委员会期望到 2014 年能实现。一旦网络电话被大量部署，其他远程信息处理服务，例如交通信息，也能够被置入和影响现有的网络电话设备。

目前标准制定的浪潮将帮助进入 M2M 的下一个阶段（“过渡”），这一阶段水平结构将大量被部署，所有权的总成本为 B2C M2M 应用的出现提供了诱人的价格模式。这个过渡阶段明显从美国、欧洲、亚洲不同的鼓励政策中受益，他们旨在资助研究、原型项目和促进被用来作为全球部署基础的互操作性标准的发展。

1.3.2.2　政府鼓励措施对 M2M 标准的影响

网络电话是一个典型的标准已经被专门发展去回应监管要求的例子：3GPP（第三代合作伙伴计划）已经为满足网络电话的需求开发出了两种标准（3GPP TS 26.267：“网络电话数据传输；带内调制解调器的解决方案；一般说明”和 3GPP TS 26.268：“网络电话数据传输；带内调制解调器的解决方案；ANSI-C 参考代码”）。这两种标准通过蜂窝语音通道和 PST 网络从车载系统（IVS）到公共安全应答点（PASA）都为事故消息可靠的传送指定了网络电话带内调制解调器。

欧盟委员会已经发布了智能计量的授权［M/441］，请求 CEN、CENELEC 和 ETSI 这三个欧洲标准化组织（ESO）提供一套部署可互操作的智能计量系统的标准。EC 授权同样为所需要标准的交付设定了一个目标日期，给予他们的交付以相当大的时间压力。智能计量授权已经被 ETSI M2M 技术委员会作为了刺激因素和一个主要的用例，他们的成员已经快速地同意了不去对智能计量本身创建另一个垂直架构。已经采取方法去处理授权需要［M/441］，仅作为广大 M2M 应用程序需求的一部分，这样就为水平架构（不同 M2M 市场部分可再次使用的能力通过公开 API 向 M2M 应用揭示的模型）产生了一强有力的工业推力，作为唯一稳定划算的模型。

在美国，作为美国复苏与再投资法案（ARRA）实现计划的一部分，美国国家标准与技术研究院（NIST）获得了来自美国能源部 1000 万美元的可用资金去为美国电力系统帮助开发一个综合的全国可完全互操作的智能电网框架。因此，美国国家标准与技术研究院已经开发出了智能电网框架（NIST SG-FW），它为智能电网提供了概念性的参考模型去识别领域、角色和接口，定义 17 条优先行动计划（PAP）。这些 PAP 的目的是为了评价那些迫切需要决议去支持一个或者多个智能电网优先区域标准的差距。PAP 指定了一些组织，这些组织已经同意用特定的交付

物去完成确定的任务。最后，目标是向制度标准组织完成必要的意见书，以便为美国智能电网部署递送一套连贯的标准。特别要注意互操作性（通过建立 NIST 智能电网互操作性座谈小组），这被［NIST SG-FW］看做是保护智能电网投资的一种必要手段：

各种智能电网元件的部署，包括配电线路上的智能传感器、家里的智能电表、广泛分布的可再生能源的资源，已经开始起步，这将作为美国能源部（DOE）智能电网投资补助和其他鼓励政策促进的一个结果，例如，为可再生能源再生项目提供的贷款担保。没有标准，用相当大的公共和私人投资发展或完成的技术就有可能被过早的废弃或是在没有必要措施确保安全的情况下完成。

（NIST 智能电网互操作性框架）

1.4 M2M 标准

不像 ICT 的其他几个部分，也许能不管标准的缺失去部署操作性系统，但几个 M2M 市场部分需要强大的标准去确保长期投资安全。对几个 M2M 应用来说，包括智能计量或智能电网，期望安装的设备能够部署超过 20 年。尽管这样长的时间对传统电话公司的部署可能不切实际（至少不寻常），但是通过公共事业部署的基础设施有很长的部署周期，这可能会戏剧化地影响它的设计和今后相关的标准。

尽管人们普遍认为市场仍然缺少 M2M 标准，但这种情况已经演化了，虽然根据标准部分，M2M 标准的成熟度依旧在改变。现在什么需要做，在那个技术和地理领域已经变得相对清楚了。

1.4.1 选择哪一个标准

需要 M2M 标准的不同领域被广泛分类如下。

1.4.1.1 数据模型

数据模型明确地决定了交换数据的结构，主要在 M2M 应用程序之间，并且还有与 M2M 系统中其他实体的。最终标准化数据模型使用所依赖的逻辑就是如果使用同样的数据结构去存储和接收数据，那么不同的应用程序就能够以一个可互操作的形式交换数据。M2M 数据模型是应用程序和特定的业务逻辑。不用说，为测量仪乱写的数据模型将不会像设计用来报告关于病人健康监控器情况的传感器一样有用，这种测量仪设计用来向实体应用程序报告关于消耗的数据。

1.4.1.2 M2M 区域网络

M2M 区域网络这个术语第一次使用是在 ETSI TS 102 690 技术规范［TS 102 690］。M2M 区域网络是一个通用的术语，指的是能够为连接到同一 M2M 区域网络的不同 M2M 设备之间提供物理层和 MAC 层的连通性或者通过路由器或网关允许

M2M 设备连接到公共网络的任何网络技术。M2M 区域网络的例子包括无线个人局域网（WPAN）技术，例如 IEEE 802.15.x、ZigBee、KNX、蓝牙等，或者本地网络，例如电力线通信（PLC）、仪表总线（M-BUS）、无线仪表总线等。

尽管几个 M2M 区域网络是基于无线射频技术，但是其他有线技术仍然在被考虑。最著名的一个超越 PLC 的例子是 G.hn 家庭标准［G.hn］，它被设计的目的是提供多个概要文件去调整多媒体/接入带宽应用程序和低复杂度/低带宽终端。选择后者很自然是符合 M2M 应用的，例如家庭能量管理。在写本书的时候，ITU-T 第 15 研究小组启动了称为 G.hnem（家庭网络能量管理）的工作，去详细说明 G.hn 是怎样能被用于智能电网应用的，例如高级计量架构（AMI）［G.hnem］。

如上所述，对 M2M 区域网络设计的关键要求与 M2M 设备本身的属性直接有关，例如：

- 低 CPU；
- 有限的内存；
- 电池操作的，低功率；
- 低成本；
- 小尺寸（对电池尺寸有进一步的约束）。

因特网工程任务组（IETF）已经为具备以上一个或几个条件资格的设备采用了这些设备约束术语。约束设备为设备支持的通信协议提出了新的、具有挑战性的需要。举个例子：人们常常希望电池操作 M2M 设备能够拥有 10～15 年的电池寿命。实现的唯一办法就是当不需要传送或接收数据时，设备通过自身改变进入睡眠模式。例如，像这样的网络应用不能依赖于设备的一直不断可用、能够发送或接收数据。例如为处理约束设备，基于 IP 通信协议的改革，包括 IETF 6LoWPAN（低功率和有损网络上的 IPv6）工作组所做的工作。6LoWPAN 工作组已经定义了封装和首要压缩机制让 IPv6 数据包在基于 IEEE 802.15.4 的网络上发送和接收。IEEE 802.15.4 最大传输单元（MTU）被限制在 127B。考虑到顶部框架和可选安全报头，除非上层协议被优化，不然为上层留得非常少，这就是 TCP/IP 和应用有效负荷。实质上，6LoWPAN 的工作是让 IP 一直被用来约束设备，一个理想的特性是允许基于 IP 的端对端通信。

1.4.1.3　M2M 接入和核心网络优化

与已经定义了专门（常常相互矛盾）标准的 M2M 区域网络不同，M2M 的运行不需要设计更进一步的接入和核心网络。为了处理额外的 M2M 业务量，远程通信运营商认为要完成接入和核心网络的改善和提高。特别地，提供基于电路的服务（也就是语音或短消息服务）和数据服务的蜂窝网络已经为了个人通信被优化。在最初的 M2M 服务部署阶段之后，在 B2B 应用，例如遥测或快速管理的主要驱动下，蜂窝运营商认为他们的网络需要变成可行的 M2M。

这种适应性的改变的一个关键因素是 M2M 业务量的特殊属性。像已经在图1-5中 M2M 业务上标出的一样，大约所有 M2M 应用中设备的 90% 是固定的。在 3GPP 和 3GPP2 无线接入中，网络有适当的手段去跟踪设备的位置（小区或小区组）。对于很自然固定的设备，例如智能电表，不断地追踪设备位置变得麻烦，而且在空中接口消耗了宝贵的无线电资源。

多种 M2M 设备另一个显著的特点是它们产生低容量数据。例如，一个实用智能电表每小时需要产生大约 200 ~ 500B 的测量数据（也许在高峰期更频繁）。在蜂窝网络中，传输数据需要在接入网络中建立数据承载，意思是几个握手消息要在接入和核心网络中的设备与其他实体之间来来回回（为了接入无线资源、认证/安全程序、获得 IP 地址、强制承载 QoS 参数、验证等）。数据承载建立和使用后的拆卸需要超过 20 次的握手信息（但并不是所有的都是起源/终止在终点），不包括常用的 TCP 传输协议的三次握手、确认和连接释放。

很明显，蜂窝接入和核心网络没有被设计用来处理数据通信模式，与实际的应用程序负载的业务量相比，这种模式中控制平面业务量变为主导（超过 80%）。

这两个例子解释了为什么要为 M2M 通信量优化接入和核心网络。这种需要通过 M2M 中新形成的业务模式进一步被放大，这种模式中，每用户平均收入（ARPU）常常比个人通信的情况低 10 ~ 15 倍。这种新的业务模式也完全改变了，例如，如何执行计费和收费。与个人通信计费和收费由每一个设备用户执行不同，M2M 通常需要在网络应用基础上执行计费（实用后端应用、中心快速管理应用等）。一个实用的例子是为所有连接到网络运营商的智能电表传送一个单独的网络使用账单，而不是每个连接的智能电表都传送一个账单。

网络运营商和设备卖主一样已经开始了最初的工作，为 3GPP 和 3GPP2 蜂窝系统的接入和核心网络优化。可是，由于在被部署到运行的网络之前产生标准要花费时间，所以运营商已经采用了一个两步的方法去应付 M2M 业务量的增长。

- 步骤一：重新构建接入和核心网络，以便更好地适应 M2M 业务量的基本特点，同时避免了影响与个人通信相关的高收益服务。一些考虑的场景包括专用设备的部署（归属位置寄存器（HLR），网关 GPRS 支持节点（GGSN））和流量隔离。总体上，步骤一实质上是目前一套对网络结构的最佳实践，允许运营商更好地利用目前的标准和产品的工具箱。这些都是通过考虑 M2M 业务量的基本特点完成的，例如低数据、不可预测性、低优先级和突发性。
- 步骤二：根据 3GPP 和 3GPP2 中 M2M 标准的开发工作，逐渐地部署新设备、软件升级和为了 M2M 业务类型而优化网络解决方案。步骤一是一个中间步骤，而步骤二被认为是为了提供长期的方向，这对大规模增长的 M2M 业务是很必要的。

很大程度上，步骤一是原始 ad hoc 阶段的结果，这个阶段 M2M 模块已经被部署在了蜂窝网络中，被像手机一样处理。我们已经得到了一些经验，由于运营商网

络上 M2M 业务量的影响，它有时是有害的。随着时间的过去，运营商已经开始总结出 M2M 需要一个与移动个人通信服务不同的方法。

1.4.1.4　水平服务平台和相关 API

如上所述，下一阶段 M2M 业务的出现将依赖于执行一系列服务能力的水平平台的部署，这是与 M2M 应用相接触的软件模块，为了加快它们的发展、测试和部署生命周期。服务能力的例子包括设备激活、设备监控、设备定位、数据存储和水平平台（运行 M2M 服务能力）的媒介化。标准化将被用来规定一套特定的 M2M 服务能力，能够通过 API 的使用去接触 M2M 应用。

电信运营商在过去已经设计了几套 API 集合，但是它们采用和部署的水平常常遭受 IT 和应用开发商团体内部可见的和专业知识缺少的影响。今天，一个成功的电信应用的实现策略就是授权被 Web 2.0 框架刺激的 IT 友好 API 的使用，这已经逐渐变得清晰。依作者在本书中对新 API 工作成功的秘诀的观点，表述性状态转移（REST）API 在过去已经参与了 IT 行业中大规模的市场采用和建立。例如在 M2M API 的背景下，基于 REST，使用 HTTP 协议的 API 正在被 ETSI M2M 详细说明。

1.4.1.5　M2M 模块和终端的认证

认证指的是设备项目某一特点的证明（通常基于一个标准）。一般地，认证是由一些外部评审、教育或者一个独立实体执行评定的形式提供的。在运行环境中，这已经变成了一个对设备项目部署（特别是终端）很重要的需求。认证可以被分为

- 自愿监管认证。欧盟成员国为 M2M 模块授权了以下认证：RoHS、WEE/RAEE 和 R&TTE 指令，它们分别属于对有害物质、GSM 无线电频谱、电磁兼容性和低压设备危险的减少。在美国，所有设备必须遵守美国联邦通信委员会（FCC）的规则。另外通信设备必须是 PTCRB 认证。
- 自愿性认证。这通常是由运营商为部署在网络中的设备授权。全球认证论坛（GCF）运行了一个独立的认证程序，旨在确保服从 2G 和 3G 无线标准。这个程序授权设备在五个有 GCF 资格的网络上测试。

另外，某些运营商在他们的网络中为设备增加了额外的认证。

最后，认证程序的目的在于确保设备坚持特定的环境和电磁兼容性特性，而且还不能在运营网络中引起任何损害。

除了属于直接连接到一个运行接入网络的设备的认证程序外，其他几个认证程序是为了设备使用短程无线电技术存在的。最著名的几个就是 ZigBee、蓝牙和 KNX。对于 KNX（作为例子被提供），认证产品必须显示符合以下一套标准：

- 符合 ISO 9001 的质量系统；
- 欧洲标准 EN 50090-2-2（包括这些方面，如电磁兼容性、电气安全和总线产品的环境条件）和一个合适的产品标准；

• KNX 认证的第 3 和 6 卷，前者是一个 KNX 协议特征的工具箱，后者根据上面提到的工具箱列出了 KNX 栈的允许概要；

• 关于标准化数据形式和（可选择的）一致功能块的 KNX 互通需求。

像 M2M 标准的发展一样，认证程序同样被期望发展，去处理这种演化。

1.4.1.6 M2M 标准化组织生态系统

几个标准化组织聚焦在 M2M 的一个或者几个方面，使得有时不可避免地复制。详述 M2M 周围的不同主动性几乎需要一本关于它自己的书。当涉及多种标准存在的 M2M 区域网络和应用数据模型时，这就特别真实（本书第 2 部分将致力于描述这两方面）。

图 1-7 提出了一些 M2M 区域网络例子，即

• ZigBee 联盟。一套根据 IEEE 802.15.4，使用低功耗无线设备的专门的通信协议（也是数据模型）。应用目标包括灯开关，有室内显示的电表、消费性电子产品设备等。

• KNX。一个以家庭和建筑控制为目的建立的无线电频率标准。它被批准作为一个国际标准（ISO/IEC 14543-3）、欧洲标准（CENELEC EN 50090 和 CEN EN 13321-1）和中国标准（GB/Z 20965）。

• 家庭网格。基于被称为 G.hn 的 ITU-T 规范套件，它被设计用来在家庭环境内提供通信，利用现有的线，例如电力线、同轴电缆、双绞线。

• IETF 协议套件。基于 IEEE 802.15.4 为无线个人局域网 L1 和 L2 提供说明书，IETF 已经开发出了一套协议旨在为受限的设备带来本地 IP 支持。

图 1-7 提出了一个用于智能计量应用环境的数据模型的例子，最著名例子是设备语言报文规范（DLMS），它已经被 CEN 和 CENELEC 在欧洲层面上采用，被 IEC 在国际层面上采用。DLMS 数据模型在美国的对应是 ANSI C12.18 套件。研究 M2M 区域网络的标准化组织也时常生产垂直应用特定的数据模型。ZigBee 和 KNX 就是如此。

尽管 ETSI TISPAN 为有线 NGN（下一代网络）提供相同的一套标准，但是当它涉及服务提供者的接入和核心网络优化时，3GPP 和 3GPP2 都是蜂窝系统中自然的组织。可是，一般公认有线标准在这个区域将看到更少的活动。

3GPP TS 22.368［TS 22.368］为机器类通信（MTC）列出了一般服务需要和特别服务需要。这个规格已经被显著参与的运营商、蜂窝系统供应商、M2M 模块供应商详细阐述，并将作为 M2M 网络改善后续工作的基础。例如，与数据模型上已经做的工作相比，这个工作的成熟度是低的。

在接入和核心网络之上和之外，ESTI M2M 技术委员会和 TIA TR50 委员会在智能设备上正在发展一种服务，旨在提供服务能力去通过开放 API 显示 M2M 应用。工作组不是从头开始工作，两者都正在通过现有标准认可构建模块去寻找方法，最

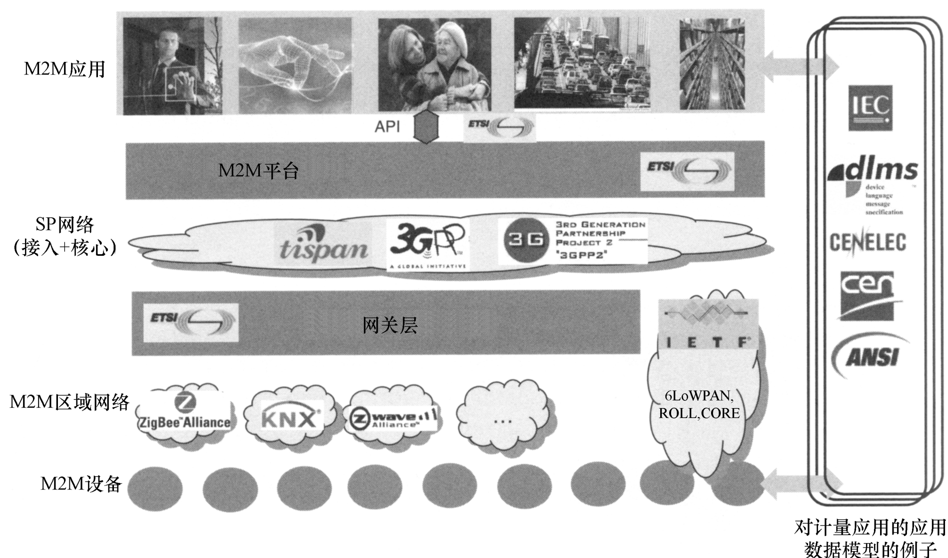


图 1-7　对 M2M 框架标准化组织的绘图

值得注意的是开放移动联盟（OMA）设备管理和宽带论坛 TR069 协议。这两种协议已经被设计用来提供远程设备配置相关功能，例如，配置管理、执行管理、错误管理和固件、软件升级。

ETSI M2M 已经为 API 工作完全认可了 HTTP/REST 方法。OMA 现存指导方针和 API 工作的重新使用已经被 ETSI M2M 专家认定为一个目标。

1.5　本书路线图

作者希望这个介绍已经获得了读者的兴趣，为下面的两部分铺平了道路。

第 1 部分（第 2 章和第 3 章）讲述了 M2M 发展的现状。

第 2 章深入描述了 M2M 业务，对于 M2M 渗透是否能够完成，通过现实的眼光深入分析了市场局面，在这个介绍中给出了目前大概的进展。市场驱动和市场障碍将在可能的转出场景中被考虑。

第 3 章：反馈和从早期市场部署中学到的教训。本章在 3GPP 商业网络上为 M2M 运营部署提供了一系列场景和相关工作配置，提供一系列学习经验作为结论和对未来标准工作的建议。

第 2 部分（第 4 ~ 8 章[㊀]）讲述 M2M 结构和协议。

㊀ 原文如此，应改为第 4 ~ 10 章。——译者注

第 4 章用支持用例驱动的方法分析了 M2M 需求去服务请求。接着介绍了高水平结构，特别聚焦在网络、服务、M2M 业务模型、M2M 端到端结构、水平和垂直结构、M2M 设备交付平台（SDP）。

第 5 章介绍了 ETSI 定义的 M2M 服务结构能力，特别地，它在服务领域、网关和设备上呈现了 M2M 的能力。在协议和 API 上做了特殊点。紧接着要考虑互操作性、基于 REST 的结构和对设备管理协议的影响。

第 6 章讲述了 M2M 接入和核心网络优化。在这个问题介绍之后，概述了在 3GPP 内问题是怎样被用各种标准化行为处理的。

第 7 章研究了 M2M 中 IP 的角色，特别是 IETF 方法。分析了 IP 协议栈（6LoWPAN）、M2M 区域网络（滚动）和受限设备（核心）REST 的路由。

第 8 章处理了 M2M 水平安全结构。

第 9 章讲述了 M2M 终端和模块。

第 10 章呈现了 SIM 卡中标准的演变和它们对 M2M 的影响。

第 3 部分（第 11 章）对未来的发展提出了一系列结论性评价和观点。

参考文献

[ARRA] American Recovery and Reinvestment Act of 2009, Public Law 111-5, http://www.gpo.gov/fdsys/pkg/PLAW-111publ5/content-detail.html.

[EISA] EISA (2007) Energy Independence and Security Act of 2007.

[G.hn] ITU-T Recommendation G.9960. Next Generation Home Networking Transceivers Foundation (Copperpair, Powerline and Coax PHY Layer).

[G.hnem] ITU-T DRAFT (2009) ITU-T DRAFT Recommendation Home Network Energy Management (Smart Grid PHY for Powerline).

[M/436] European Commission (2008) Standardisation Mandate to the European Standardisation Organisation CEN, CENELEC and ETSI in the Field of Information and Communication Technologies Applied to Radio Frequency Identification (RFID) and Systems, M/436.

[M/441] European Commission (2009) Standardisation Mandate to CEN, CENELEC and ETSI in the Field of Measuring Instruments for the Development of an Open Architecture for Utility Meters Involving Communication Protocols Enabling Interoperability, M/441.

[NIST SG-FW] NIST (2010) NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, NIST Special Publication 1108, http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

[TS 22.368] (2009) Technical Specification Group Services and System Aspects; Service requirements for Machine-Type Communications (MTC); Stage 1; Release 10.

[TS 102 690] (2011) ETSI Technical Specification, M2M Functional Architecture, Stage 2 Specification.

第 1 部分

M2M 现今发展状况

第 2 章　M2M 的业务模式

Harish Viswanathan
阿尔卡特朗讯公司，新泽西，美国

术语 M2M 非常宽泛，指的是许多不同的垂直市场、多样的通信技术和一个潜在的大的地理范围。M2M 有潜力去提升许多工业现有的过程，简单地列举几个，例如，健康护理、自动化、制造、能源、零售和公共安全。同样，依据技术，M2M 应用到了大量短距离无线通信技术，例如 ZigBee[1] 和 Zwave[2]，它通过一个更智能的网关或者路由节点连接传感器到有线技术，例如 X10[3]，连接到设计用来监测和控制电网的广域监控与数据采集（SCADA）网络，使用近场通信技术连接到射频识别（RFID）标签，连接到广域移动无线网络方面，例如，CDMA、GPRS、UMTS、LTE 网络和卫星通信网络。结果，评估目前部署的 M2M 设备数量和它们增长的潜力不是一个简单的任务。M2M 解决方法的地理范围能够是本地和全球的，例如跨国运输/航运公司穿越大陆追踪它们的船队，一个小型的、拥有远程控制设备的公寓，这个设备在本地主服务器上运行能量管理控制应用程序。除了这样一个宽的范围，在设备和控制它们行为的应用程序之间，确实有一个标准去连接到没有人类介入的通信点。

多种应用程序、技术和其他 M2M 规模使得 M2M 业务模式高度复杂。M2M 价值链有许多缺乏整合的参与者，导致 M2M 市场的脆弱。用不足的和不完整的端对端标准解决方法过多叙述部分方面和解决方法的标准进一步使市场脆弱。结果，M2M 部署的多业务模式仍然盛行，将持续好几年。

本章的结构是这样的。开始是主要垂直市场的描述和每个这些市场内提供的专门应用。接着对每一个部分用工业参与者的例子讨论了价值链的关键部分，然后是对主要市场每一部分市场规模的预测。其后，呈现了一般在广域无线 M2M 部署中看到的三种不同业务模型，包括在市场发展上几个指导方针的规定。

2.1　M2M 市场

从很大程度上，M2M 本身不是一个市场；它相当于从 M2M 通信受益的多垂直市场中的一个延伸，M2M 扮演重大角色的主要市场是医疗保健、运输、能源、安全和监控、公共服务管理（安全与交通）、零售、销售点、电子市场、建筑控制/

管理、工业自动化与控制、家庭自动化与控制，以及农业。在医疗保健、运输、能源领域，我们进一步详述了一些典型的应用和用例，以及在每一个市场中所采用技术的本质。尽管在本章中没有详述，但是其他垂直市场同样有相似的潜在应用。

2.1.1　医疗保健行业

- 远程病人监控
  - 通过广域网（WAN）获得心率、血糖水平和其他身体功能指数。
- 家居护理/辅助生活
  - 远程监控需要护理和帮助人的安全和健康。
  - 监控和对病人每日的活动发送提醒，例如吃药。
  - 通过视频会诊治疗和帮助病人。
- 资产追踪
  - 追踪价值高的资产，例如医院内的静脉泵、轮椅和担架。
  - 管理药品时，用 RFID 标记药品来消除错误。

远程病人监控在监控设备和作为网关的蜂窝电话之间特别涉及了蓝牙连接的使用，这个电话转而被用来连接广域网。

家庭护理应用在家里使用了多种传感器，用局域网（也被称为 ETSI M2M 规格中 M2M 区域网络）通信，通过一个家庭网关和宽带连接到因特网。

医疗设备的资产追踪在医院里被典型地使用，它是基于 WiFi 定位、RFID 和不定期的红外通信。

2.1.2　物流行业

- 车队管理
  - 确定车辆的位置，向个别车辆发送调度通知，向一队车辆发送关于附近某些事件的团体调度通知，从车辆上收集关于使用和维护的数据。
- 车辆维护
  - 为了主动诊断机械故障而从车辆上获得各种参数。
  - 为车辆推动软件升级，这样对汽车经销商来说就避免了昂贵的召回。
  - 汽车经销商可以推动提醒和特殊的待遇给车主关于车辆日常维护或促销优惠。
  - 电动汽车（EV）相关充电的应用，例如提供充电站的位置，管理充电过程和车内的参数，如果有的话，就生成计费的相关记录。
- 保险
  - 远程监控位置、使用数据和司机的行为数据来提供不同的保险费用，以反映司机不同的个人档案。

- 娱乐资讯
  - 向汽车提供媒体（音频、地图视频信息等）。
- 防盗
  - 如果报告为被盗或定位汽车为丢失，则远程禁用汽车。
- 紧急呼叫支持
  - 在一个事故发生和建立一个语音连接中，自动上传参数（速度、照片、位置等）。
- 导航
  - 根据特定的标准，提供方向和周边地区的信息，包括兴趣点，来优化路由选择。
- 收费
  - 在特定的道路行驶时自动支付通行费；收费可能是根据一天使用道路的时间和其他因素，如污染水平。
- 资产跟踪
  - 跟踪卡车或其他形式的交通工具里的目标。

由于车辆通信固有的移动性的要求，几乎所有的交通应用都涉及商用蜂窝网络的使用。通常，一个调制解调器被嵌入在车内，车辆使用移动通信来连接到网络中的应用服务器。

2.1.3 能源行业

- 智能计量
  - 从水或能源计量设备自动收集消费、诊断和状态信息数据。数据传达到一个中央数据库进行计费、故障诊断、分析和负载管理。
- 需求响应
  - 为了使峰值负荷最小化，调整和分发动态价格信息。
- 消费者管理应用（独立于公用事业提供者）
  - 监视个人电器电力的使用和报告给一个提供管理服务的中央实体。
- 替代能源（太阳电池板、风力等）
  - 监控、维护。
- EV
  - 充电控制、账单信息，以及电动汽车作为一个电网存储设备的使用。

能源应用使用一个混合的家庭局域网，本地通信技术，如电力线通信或到最近的变电站的网状射频（RF）网络，到处理数据中央位置的有线网络。一些智能电表也基于蜂窝无线网络。大型公用事业公司倾向于为了他们的通信需求部署他们自己的网络。

2.2　M2M 市场的接受：驱动及障碍

预计 M2M 在未来 10 年将显著增长。

- 哪些因素将推动这种增长？
- 与某些其他的技术一样，这真的是成功，或者仅仅是炒作？

应该指出的是，M2M 概念既不是革命性的也不是新的。它已经在特定的应用中使用了几十年。然而，现在不同的是横跨不同的产业大规模采用的潜力，被一些趋同的因素所推动，这似乎导致了一个“完美风暴”。尽管如此，在 M2M 市场发挥其全部潜力之前，仍有对增长的重大障碍需要去克服。

我们目前看到的主要驱动力如下。

- 降低设备和通信成本的价格。半导体和无线电技术上的进步加上更成熟的广域通信协议已经导致通信模块价格下降。在大多数国家是用语音收入来达到饱和点，为了未来的增长，网络运营商正在寻找新的领域，包括数据收入。M2M 业务一个固有的性质是交换的数据主要由大量的小型负载处理组成，这使其每字节所携带的信息有很高的利润。例如，它花费大约 20 美分发送一个 140B 的短消息，而一个每月 5GB 的数据计划要花费大约 50 美元，当进入大范围的部署时，即使这样的价格模式受到改革，每字节的数据里短消息都有 100000 倍的利润可图。网络运营商也渴望在他们的网络中尽可能多地添加机器设备用户。提供灵活的和有吸引力的定价方案去为 M2M 部署产生积极的投资回报（RoI），从而培养它们增长。
- 有线和无线 IP 网络的广泛部署。跨越不同网络类型，IP 已成为网络通信的实际标准。大多数全球通信服务供应商在国家和国际层面上部署了 IP 网络。使用相同的核心网络技术显著简化了设备和应用的部署与维护。对于大多数大型 M2M 部署，包括有线和无线设备，一个单一处理所有设备的应用意味着更低的总体拥有成本，将导致更快的投资回报。
- 商业网络提供的无处不在的覆盖范围。在过去，公司不得不依靠他们自己的网络来满足 M2M 应用的需要。早期的商业网络既没有在所有地理区域提供足够的覆盖，也没有满足一些 M2M 应用所有苛刻的性能要求。随着有线和无线宽带的出现，通过多个运营商的选择，现在的网络到达比以往更容易获得。提供良好延迟和服务质量（QoS）的先进技术可以被在网络成本中没有大量前期投资的公司使用。
- 清晰的监管要求和绿色技术投资。全球变暖已经创造了一个新的认识，那就是需要更环保的技术。世界各国政府在能源的分布和消费上都在提高效率。这很好理解，信息与通信技术（ICT）通过仔细监测和控制能源消费在减少碳排放方面能

扮演一个重要角色。远程监视和控制是一个关键的 M2M 技术的应用，这推动了在绿色技术上 M2M 的使用。

对于 M2M 解决方案大规模推出，以下是一些主要的障碍。

- 众多的不完整的标准导致市场分裂。有大量的标准解决相同的问题，其中没有一个是足够完整的，能去应对端到端解决方案的需求。例如，ZigBee、Zwave、无线 HART、IETF 6LoWPAN/ROLL，所有都是处理传感器和一个网关或路由器之间短程通信的。应用级的标准存在于一些垂直应用上，例如医疗保健和智能计量，但又有多种实现选项。对于一个消费者来说，把一个现成的传感器从零售商店添加到他们的家庭网络，还希望它和来自一些供应商的现存家庭控制应用一起工作，这显然是不可能的。大多数应用使用专有技术连接到它们的设备。对大量的系统集成工作是如此的要求，这导致了更高的成本。由于缺乏一个发明新概念的总体框架，创新也受到了阻碍。
- 全球监管障碍。因为不同的国家有不同的规则，所以监管也可以延迟全球部署。监管可能是在应用层面，例如在如何获得、存储和传播医疗保健数据上，甚至在通信层面。此外，认证可能不得不在每一个国家或地区被获得，导致更高的成本。
- 安全和隐私。M2M 通常要涉及人们自己项目中数据的收集，并且经常在自己家里。从隐私的角度，有一种很自然的趋势去反对数据的收集。例如，如果所有人们买的东西都被射频识别系统标记，包括他们的钱包，这就可以提取到人活动和消费行为的信息。由于隐私问题，一般对这项技术的反对可能会延迟或甚至阻止许多 M2M 部署。
- 载体的可移植性。对于广域无线 M2M，许多公司的一个关注是无法轻易更换运营商。几种类型的设备都被部署有一个焊接的不能移除的 SIM 卡，因此阻止了任何网络运营商的改变。即使 SIM 是可去除的，派遣人员在成千上万的 M2M 设备中改变 SIM 卡，这将是非常昂贵的。这使得公司很难在设备的生命周期结束之前更换运营商，这在某些情况下可以是几十年。对这个问题潜在的解决方案涉及多网络经营者，它们与多个网络运营商有带宽关系。然而，随着网络运营商直接接近公司客户，缺乏可移植性就可能是一个障碍。
- 网络运营商和公司不匹配。许多 M2M 服务的生命周期可达 15 年，例如，对于智能电表的部署。这意味着公司，如公共事业设备公司，希望网络运营商保证特定技术很长一段时间的可用性。然而，这对网络运营商而言是困难的，为了更好地使用有限的可用频谱，这需要经常升级技术。因此，在包含服务部署的各部分之中，有一个在技术期望上潜在的失配。
- 技术挑战。最后但并非最不重要的是，当 M2M 快速发展时，很可能会有许多技术挑战必须去克服，例如：

– 设备管理；
– 网络可伸缩性；
– 提供者网络上的设备身份验证（初始和重复请求）；
– 用户网络和应用策略；
– 计费规则。

2.3　M2M 价值链

图 2-1 显示了涉及一个广域网典型部署的价值链，比如在交通运输领域。图 2-1中公司的名单被提供作为一个示例，并不是全面的。该价值链的设备终端包括嵌入模块机器的制造商。例如，汽车是一个连接到汽车应用的“机器”，或电表是一个嵌入通信模块的“机器”。这台机器包括传感和驱动能力，它可能是作为通信模块的同一个集成电路的一部分。对于这部分的价值链参与者是多种多样的，取决于特定的垂直行业。

下一个重要的部门是通信模块或芯片制造商。模块包括蜂窝模块以及短程通信技术，如 ZigBee 或 Zwave。在这一类中也包括独立的调制解调器或网关设备的供应商或厂商，可以直接或通过另一个本地通信接口附加传感器设备到这些设备上。在图 2-1 中提供了一些提供 M2M 通信模块公司的例子。这些公司中的大多数为了移动蜂窝手机的连接提供模块。

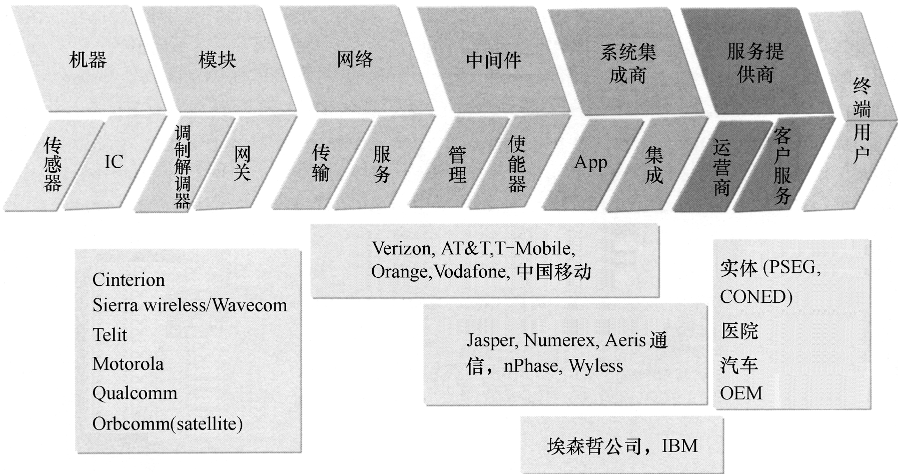


图 2-1　一个典型的 M2M 价值链

用于 M2M 中的商业网络正变得越来越受欢迎。当商业网络被使用，从提供连通性和设备与基于互联网应用之间的数据传输角度来看，网络运营商或通信服务提

供商就形成了价值链的核心。大型公司如电力公司，可能部署自己的基础设施来传输他们自己的数据。在这种情况下，价值链中的一些组件被吸收进公司或服务提供者里面。同样，当解决方案的地理范围仅限于建筑物内部，那么这里可能就没有参与的网络运营商，因为通信将涉及建筑物内的局域网。

中间件包括大量的 M2M 服务功能，它们是水平的，适用于许多不同的应用。一些功能是设备管理、诊断、消息传递功能，比如短消息服务、自动化设备的激活和服务提供。中间件是一个 M2M 服务平台典型的部分，既通过大型网络运营商提供，也通过特殊 M2M 提供商提供，如 Jasper 无线公司，Wyless 公司，或 Aeris 通信公司。一些网络运营商与平台提供者成为伙伴关系，在托管软件作为服务模型方面，平台提供者为网络运营商提供平台。

系统集成商就是汇集所有端对端解决方案需求功能的公司，并执行硬件和软件不同的解决方案的集成。他们雇佣必要的分包商去建立专用的应用软件。通常情况下，由于每个 M2M 解决方案往往都是为即将到来的特殊应用专门设计的，所以需要做大量的集成工作。系统集成商经常选择机器厂商、网络运营商、M2M 平台提供者代表终端服务提供者。系统集成商的例子包括诸如埃森哲和 IBM 这样的公司。

应用服务提供商的实体，他们提供给其客户 M2M 服务。客户通常是消费者或提供服务公司的员工。如果可以，服务提供者将对 M2M 服务的日常运营和客户服务与收费负责。对于远程病人监控解决方案，服务提供者通常是医院或诊所。医院的 IT 部门将向医院的医生、护士和病人提供服务。对于智能计量，服务提供者将是公用事业公司。在某些情况下，服务提供者可以把服务外包给一个托管服务提供者。

多种在价值链上面的变化是可能的，事实上经常在市场中观察到。网络运营商正越来越多地提供他们自主开发的解决方案或一个合伙中间件或 M2M 平台。他们也参与系统集成，有时也与合作者一起提供预先集成的解决方案。对于消费者应用，如家庭自动化和控制，网络运营商可以提供终端用户服务。另一个变化是通过应用服务提供商私有网络的使用，在这种情况下，网络运营商没有参与其中。进一步的变化是在应用提供者，也包括中间件或 M2M 平台本身。这是真实的，例如，对于亚马逊的电子阅读器服务。经销商也可能参与在价值链的各部分中。

2.4 市场规模预测

M2M 市场规模的估计通常首先估计 M2M 设备的数量。正如前面所讨论的，估计设备的数量是棘手的，因为 M2M 巨大的范围和每个市场不确定的增长潜力。它

基本上包括来自各行各业的潜在的应用，每个都有自己适用的时间表。以下是一些对设备数量普遍的市场预测：

- 到 2013 年有 1 万亿连接的设备；
- 到 2014 年有 4.15 亿移动互联网设备；
- 到 2020 年有 500 亿联网设备。

为什么这些预测会如此不同？答案在于确切知道预测中到底包含什么。在第一个预测中，很有可能是很短距离的设备如 RFID/NFC 包括在总预测内。因为会有大量的 RFID 可能从互联网的任何地方被读到，所以根据这个预测，设备的总数量是非常大的。第二个预测可能仅包括短距离设备，例如基于 IEEE 802.15.4 技术的设备、蓝牙、基于 IEEE 802.11 的局域网、网状网络和蜂窝设备。最后一个预测仅包括直接连接到蜂窝网络的设备和网关，关键的一点是所有预测的共同点是非常巨大的 M2M 市场潜力。

依据美元价值，对市场规模而言，我们参考 Beecham 2008 年的报告。图 2-2 显示了市场大小分为四大类：

- 互联网实现指的是价值链的模块和设备组件。它包括了允许连接到互联网的调制解调器和网关。
- 市场的网络部分是指从 M2M 设备位置到应用的位置比特值传输中的价值。
- 图例中的系统应用是指中间件，它跨越所有 M2M 应用程序，包含了常见的功能，如控制和诊断、设备管理、位置、状态和跟踪信息。在图 2-1 中，这包括了价值链图中的中间件组件。
- 最后，增值服务通常指在价值链的中间件右边的所有其他组件，包括服务，如系统集成、软件应用开发、日常维护的运作和提供相关服务的应用程序给终端用户。

应用或服务部分的总价值被分解成了不同的垂直行业。以 10 亿美元计，图2-3 显示了从 2008 年到 2012 年对每个主要的垂直行业市场大小的估计，这也能从 Beecham[4] 同样的市场报告中得到。这表明零售、安全、交通运输、能源都是潜在的最大市场。医疗保健，在 2012 年相对小一点，是在最快增长市场部分中间。应该注意到，这些数据包含了所有基本的网络技术，那就是局域网、广域网、有线和无线。

2.5　商业模式

尽管预测市场规模相当大，但 M2M 仍处于初级阶段。在今天的市场中，许多不同的业务模型和资金流动是普遍的。一个典型的 M2M 部署可能涉及，也可能不涉及商业网络运营商或通信服务提供商。对于一个连接中的汽车，例如，典型的带

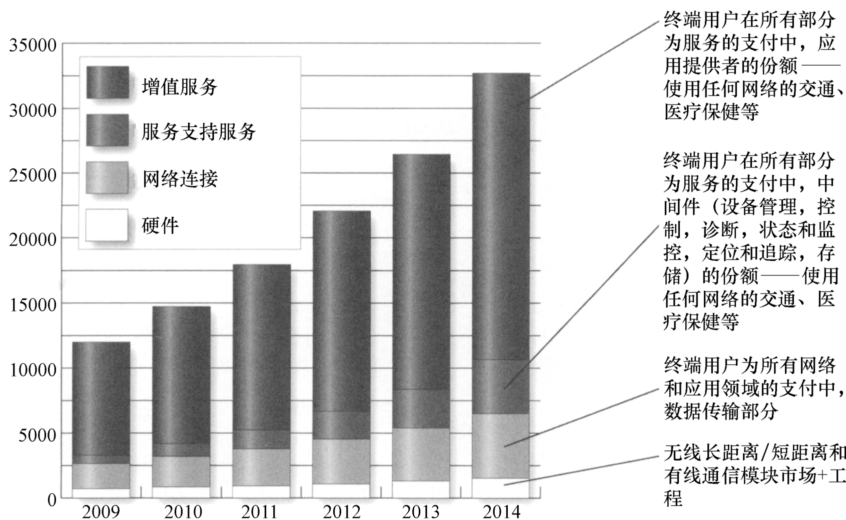


图 2-2 对价值链中不同角色的估计 M2M 收入绘图（Beecham Research 允许复制）

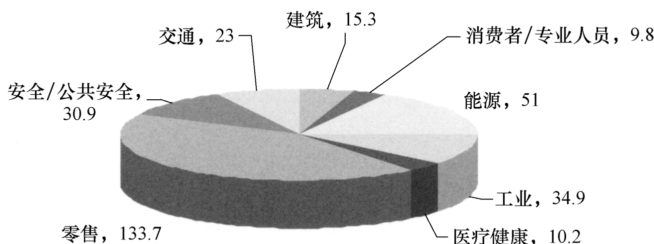


图 2-3 垂直部分的 M2M 市场大小
（10 亿美元，Beecham Research 允许复制）

有 SIM 卡的嵌入式调制解调器被安装在汽车上，用来连接无线网络运营商提供的服务。还有其他的模型一点也不涉及商业网络运营商。例如，除满足公用事业公司的其他需要之外，大型公用事业公司可能部署他们自己的网络用于 M2M。另一个可能性是一个 M2M 网络可能完全位于一个大公司的建筑里，如医院或一个大的度假酒店。集中注意力在广域 M2M，其中有数据流通过一个商业网络运营商或通信服务提供商，我们在本节中说明了三个不同的模式。这些模式是被当做 M2M 业务性质的例子来说明包含的复杂性，但它们也绝不是详尽的。

2.5.1 网络运营商或 CSP 主导模式

在这个模式中，通信服务提供商（CSP）在 M2M 解决方案中起着核心作用。CSP 企业客户用向部署的一个 M2M 服务请求的方法直接接近 CSP。CSP 扮演了一

个系统集成商的角色，并通过它的合作伙伴，为企业客户提供一个端到端解决方案。CSP 也可能随意地选择系统集成商的服务。CSP 从其合作伙伴中选择一个设备供应商和应用软件开发人员来为选择的特定设备编写应用程序。CPS 可能有他们自主开发的 M2M 服务平台或可能与平台提供商之一合作，如 Jasper 无线，在一个托管模式的基础上提供平台服务。

价值和资金流量如图 2-4 所示。企业客户为了初始解决方案开发和部署向 CSP 支付，也为正在进行的网络和使用的服务支付。如果有一个涉及其中，CSP 反过来为了设备向设备供应商付钱，为应用软件向一个应用软件提供商支付，与一个 M2M 服务平台提供者分享持续的收益。此外，如果与一个有关，可能会有资金流向系统集成商。

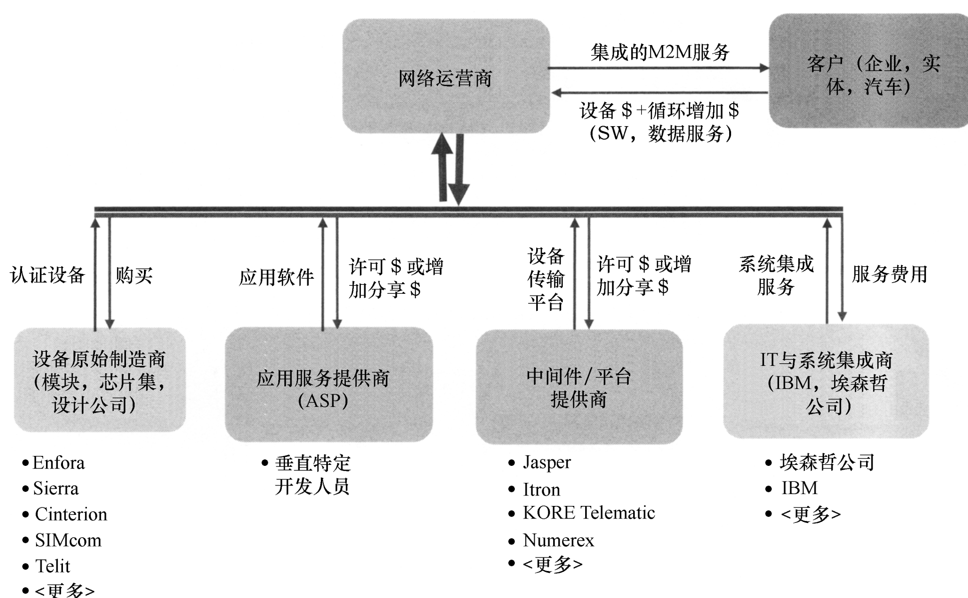


图 2-4　网络运营商或 CSP 主导模式

作为这个模式的一个例子，一个小的公用事业公司可能有一个需求去读取它的计量仪表和产生计量数据。例如，AT&T 公司与 SmartSync 公司合作为公用事业公司提供这样一个解决方案。

2.5.2　MVNO 主导模式

在早期的 M2M 中，M2M 设备部署的数量对于移动网络运营商充分参与是不足够的。它们满足专门的 M2M 移动虚拟网络运营商（MVNO）的带宽协议。MVNO 反过来在 M2M 生态系统中发挥了核心作用，去直接与最终企业客户相互作用。

MVNO 也通过他们的平台和设备合作伙伴促进了部署。他们有时也为他们的客户开发应用程序。图 2-5 还显示可能涉及的系统集成商。

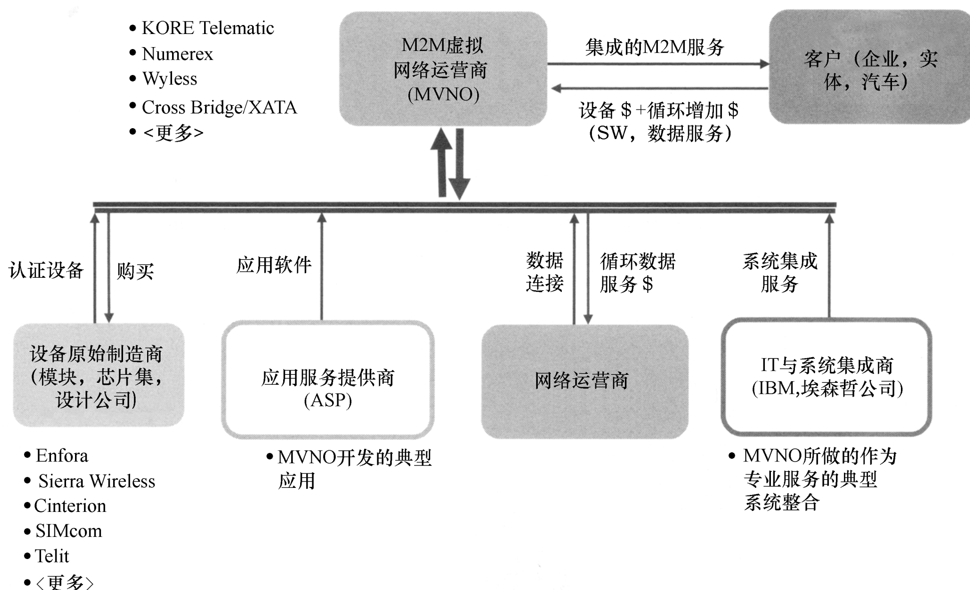


图 2-5 MVNO 主导模式

2.5.3 企业客户主导模式

讨论的最后一个模式，如图 2-6 中，M2M 客户或服务提供者本身扮演了领导角色。这是大型企业部署大量设备的典型例子。公司为了通信需求参与了与选定的网络运营商的协商，还为 M2M 服务提供了一个平台供应者或 MVNO。这个 MVNO 反过来可能提供有关的 M2M 模块或设备。这个模型的一个例子是亚马逊的电子阅读书。亚马逊已经集成了 3G 模块到其电子书中，为了在无线网络中递送书籍和其他信息，他们与 AT&T 达成带宽协议。终端消费者并不需要为了电子书而向 AT&T 订阅。亚马逊已经部署了一个用于此目的的 M2M 平台。

2.6 M2M 业务指标

如何才能衡量 M2M 业务的成功呢？当然，这对 M2M 应用提供者是完全不同的，如网络运营商的公司。网络运营商习惯上用每用户平均收入（ARPU），或者每订阅的基本月收入和流失率，去衡量消费者语音和数据的连接。对于 M2M 来

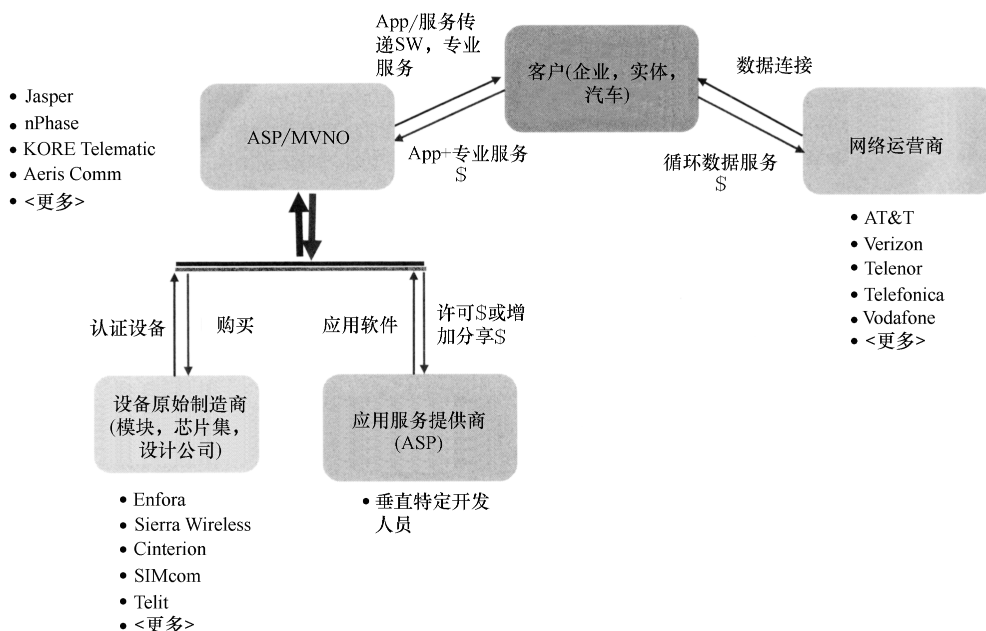


图 2-6　价值和资金流动的例子

说，相同的度量标准可能不完全适用。对于传统服务，每月平均 ARPU 是 50 美元左右，而 M2M 连接的 ARPU 要小得多，大概是 5 美元左右，尽管在最好的情况下，对于一些数据密集型应用，ARPU 可以高达 150 美元，比如数字标牌。然而，简单地看 ARPU 可能产生误导。它未能抓住的事实是客户获取、保留成本，甚至是运输成本，都比 M2M 连接小得多。即使 ARPU 很小，利润仍然相当高。此外，M2M 业务的存在可能真的是网络运营商的一种方式，去接近公司赢得更多的企业业务，比如 WAN 或 VPN 和云服务。从战略上讲，这对尽可能多的公司存在于 M2M 空间是重要的。

从公司的角度来看，主要的 M2M 指标是投资回报（RoI）和其他一些无形资产，如改善他们能向客户所提供的帮助。另一个与 RoI 相关的关键指标是看到回报所花费的时间。因为完成部署所需要的时间和所看到的真正好处的影响，许多 M2M 项目在评估阶段就被抛弃。

2.7　市场演变

目前市场发生的一个根本性的变化是无线网络运营商变成关键角色。在过去，由于无线运营商主要关注语音业务，他们很少关注 M2M 市场。无线 M2M 市场对

于网络运营商仅仅意味着向 M2M 专门的 MVNO 批发带宽协议，而他们反过来则服务企业客户。由于语音收入的饱和，无线运营商将注意力转向数据收入来弥补财政赤字，尤其是 M2M 数据收入，它提供了高利润率和客户的低流失。大多数运营商现在已经创建了专门的 M2M 销售部门去接近 M2M 企业客户。加上这一点，他们通常与托管 M2M 服务平台提供者达成伙伴关系，而这些提供者能够使许多设备管理和结算流程自动化。一些无线运营商也已经建立了自主开发的平台来满足他们 M2M 客户的需要。下一阶段的演变可能是供应商提供、网络运营商拥有并经营的更多标准化平台的开发，来作为网络基础设施的一部分。随着市场变得庞大，这将允许运营商从他们竞争者的产品中区分他们的产品和巩固他们的附加值。

另一个 M2M 市场的演变可能受新兴标准的推动，如 ETSI 技术委员会 M2M 标准。随着网络运营商和厂商的重要参与，标准的提供将建立一个框架，在这个框架之上，一个生态系统可以聚合，随后创新开发出新的解决方案。它把 M2M 从一个有不同实现的垂直市场搬到了一个有多个应用运行其上的更加横向的平台。这应该能降低成本，从而使更广泛的适用成为一种切实存在的可能。

参 考 文 献

1. ZigBee document 053474r17, ZigBee specification release 17, ZigBee Technical Steering Committee.
2. Zensys, SDS10242, Software Design Specification, Z-Wave Device Class Specification.
3. The X.10 specifications can be found under this link: ftp://ftp.x10.com/pub/manuals.
4. Beecham research, Worldwide Cellular M2M Services Forecast Market Brief, 02.08.2009.

第3章　早期M2M部署的经验教训

Samia Benrachi-Maassam
布依格电信公司，巴黎，法国

3.1　引言

当前M2M部署的快速增长催生了几个目前网络服务提供商面临的运作挑战，那就是他们安装的基础设施已经主要为了个人通信被设计和优化。本章的目的是分享一些最重要的发现和经验教训，以及描述一组目前为了应对当前M2M的增长而在网络构架方面的最佳实践。

虽然M2M设备可能使用几个通信技术，包括短程RF、有线和蜂窝2G/3G/4G，但是本章将集中探讨使用2G和3G通信模块连接到移动网络运营商（MNO）的设备。蜂窝技术提供了几个特征去匹配M2M市场几个部分的需求。这些包括可用性和地理覆盖范围、低延迟和高水平的安全。此外，网络运营商，特别是移动网络运营商，对于M2M的部署来说正在成为一个可信的伙伴，他们越来越多地提供新的超出基本连接性和活动的增值服务，包含一个模式，在这种模式中他们成为了M2M服务提供商。

移动网络运营商部署M2M面临的第一个挑战是运行大量的M2M设备的能力，这些设备在不影响个人通信服务的情况下表现出不同业务量的特点。毫无疑问，这种部署必须使用现有的基础设施和技术，然后应该利用资本性支出（CAPEX）和MNO投资运营成本（OPEX）。这样一个挑战要求对服务需求，以及对每个目标市场部分的业务量特点有一个清楚的了解。本章剩下的部分结构如下所示。首先，随着作出技术架构的选择来解决不同M2M应用需求，提供一个运作M2M部署的概述。其次，总结一些与M2M相关的挑战，以及介绍一些初始的架构优化机制。最后，本章提供了从早期M2M服务部署中得出的主要教训的总结。

3.2　早期M2M运营部署

3.2.1　引言

本节描述多个使用现有MNO网络的M2M运营部署示例。这些例子被选是为

了演示目前对数据收集（或交换）各种可能的技术选择，以及设备触发。设备触发是指 M2M 服务器[一]通过 M2M 设备用来触发一个数据承载[二]建立的机制。虽然对于每一个设备持续运转和拥有一个永久的分配 IP 地址来说，它可能是令人满意的，但由于网络资源的使用和能量损耗，这样的设置是昂贵的。因此，对于传输非常少量数据的设备来说，利用电路交换（CS）域的服务，比如 SMS，可能更高效。粗略地讲，以下部署的例子强调了本节所阐述的不同技术选择：

- 数据收集和交换可以通过执行：
  - **CS 域服务**，例如 SMS 和电路交换数据（CSD）[三]。使用 CS 域更多的是针对偶尔发射非常少量数据的 M2M 应用部署的例子。
  - **分组交换（PS）承载**。使用 PS 域更多的是针对需要传输相对大量数据或要求较低网络延迟的应用。通用分组无线业务（GPRS）承载可以被建立在一个永久的基础上（总是运行）或在 M2M 装置的主动性之上，既是定期的，又是基于触发器的，如数据可用性，或一个警报。
- 设备被 M2M 服务器触发可以通过执行：
  - **发送一个特定的 SMS 到设备**：该设备然后通过建立一个 GPRS 承载反应，也指的是分组数据协议（PDP）环境激活。
  - **一个无应答语音电话**：通常，M2M 服务器触发一个通向 M2M 设备语音电话的建立。M2M 设备识别主叫用户的数量，用无应答语音电话触发一个 PDP 环境的建立。
  - **网络请求的 PDP 环境激活（NRPCA）**：这允许网络为了 M2M 服务器而去建立一个 PDP 环境。这样一个特性使得不需要发送 SMS 或者一个无应答语音电话的解决方案。但是，由于其内在的技术限制，它没有被广泛部署在运行网络中。正在进行的 3GPP 标准工作旨在优化 NRPCA 机制（参见第 6 章）。

图 3-1 提供了一个使用 SMS 或无应答电话技术的设备的概述。

- 步骤 1 和 2：M2M 服务器发出一个语音电话（通过 MSC-S）[四]或发送 SMS 到 M2M 设备（通过短消息服务中心（SMS-C）。然后传送请求（语音电话或 SMS）到 M2M 设备。
- 步骤 3：M2M 设备认识到需要建立 PDP 环境。

[一] 在剩余的章节中，术语 M2M 服务器和 M2M 程序服务器可以互换使用。

[二] 一个数据承载是由允许数据交换的连接网络定义的。通常，以下术语被用于一个 MNO 中，分组数据协议（PDP）环境、通用分组无线业务（GPRS）承载和分组数据网络（PDN）连接。

[三] 见下文对 CSD 服务的解释。

[四] MSC-S 指的是移动交换中心服务器，SMS-C 指的是短消息服务中心。

● 步骤 4：建立 PDP 环境。结果 M2M 设备获取了一个 IP 地址，能够用 TCP/IP 协议与 M2M 服务器通信。

● 步骤 5：M2M 设备与 M2M 服务器交换数据。

注意，设备触发可用于结合一个周期性 PDP 环境的承载建立。设备被配置用来建立周期性连接（周期性通过配置的方法设置在 M2M 设备中）。因此，设备触发被用在该 M2M 服务器需要接入 M2M 设备的时候，同时，例如，测量数据的定期报告发生在主动的 M2M 设备上。

GPRS 网络部署之前，为了 M2M 应用，CSD 已经作为数据交换技术被普遍部署。CSD 是为 GSM 系统开发的数据传输的原始形式。CSD 技术允许一个 9.6kbit/s 的上行和下行带宽，这对早期/几个 M2M 应用程序（发送计量数据、气罐位置的信息等）是足够的。

本节的其余部分提供了一些关于上述机制的工具箱，可以用来解决不同 M2M 应用需要的示例。

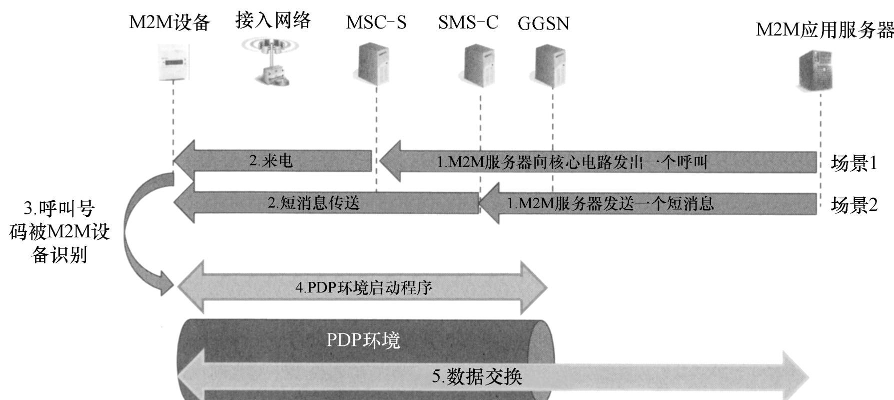


图 3-1　设备触发型通信模型

3.2.2　早期 M2M 运营部署举例

3.2.2.1　车辆追踪

基于 M2M 应用的车辆跟踪，比如车队管理和按里程付费的汽车保险，依靠 MNO 的能力去计算和使得跟踪车辆的位置对 M2M 应用服务器是有效的。在其他情况下，M2M 终端使用一个通信网络承载向 M2M 应用服务器报告位置信息。在这个特定例子中，有两类可以交换的定位：

● GPS 定位。提供更准确的定位，但授权一个 GPS 天线的部署，可能不是在所有的条件下都起作用。

● 网络定位。或是基于服务一个特定终端的基站台而提供（但提供一个不太准确的位置）或是基于三角测量技术来估计，这个技术是考虑从基站台测量的信号强度。

如图 3-2 所示，M2M 服务器从定位平台请求 M2M 设备的地理位置（步骤 1），地理定位平台使归属位置寄存器（HLR）投票去联系控制 M2M 设备的 MSC-S（步骤 2）。在步骤 3 ~6 中，地理定位服务器请求 MSC-S 浏览所有的小区，在这些小区里 M2M 设备有可能被安置来提供 2G/3G 小区身份信息。根据预配置映射表，定位平台然后转换 2G/3G 小区身份为一地理定位位置（步骤 7），地理定位信息接着通过一个预先建立的安全 VPN 通道被传输到 M2M 服务器（步骤 8）以确保隐私。注意，定位平台可以使位置信息用于多个 M2M 服务器，它们对于 M2M 设备具备适当的权利（步骤 9）。

当 M2M 应用服务器需要时，GPS 和网络位置信息以一个互补的方式可以被用来提供准确的位置信息。GPS 位置信息，比如，可以用在发生车祸或其他紧急情况时，来向救援服务提供准确的信息。

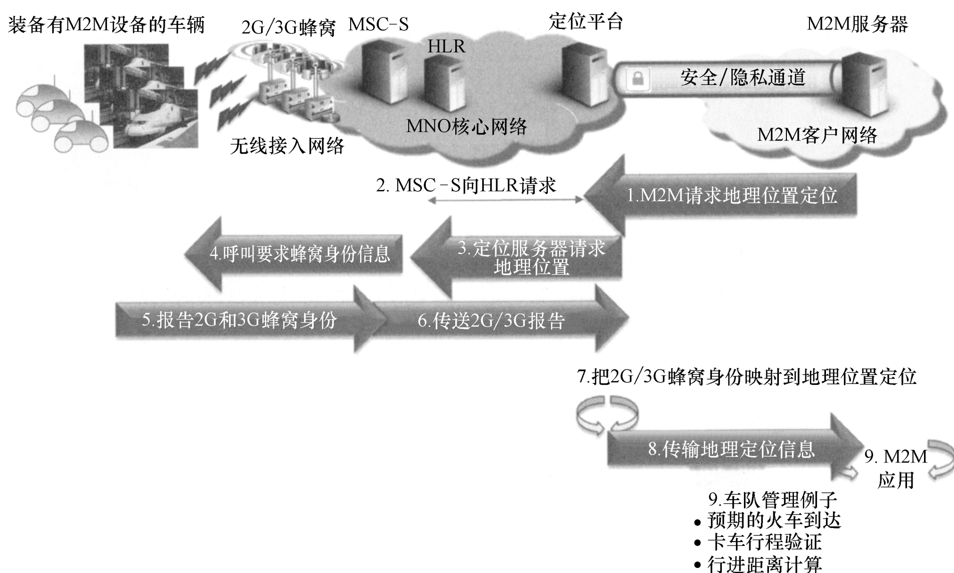


图 3-2　车辆追踪 M2M 应用基本规则

3.2.2.2　智能遥测

智能遥测允许来自电表的各种数据实时收集，例如提供温度、能耗或污染水平的那些电表。在本节中，描述了以下部署场景：电子智能计量和气罐监控。

在智能计量的例子中，M2M 设备被配置来按时间表定期报告计量数据，例如，

每 3h 智能电表将向 M2M 服务器报告计量信息。为了定期报告，在当前部署中采用了两种可能的解决方案：

- SMS 解决方案：用 SMS 报告计量数据。
- GPRS 解决方案：建立了 GPRS，然后通过 TCP/IP 报告计量数据。

基于 SMS 或基于 GPRS 的解决方案的选择通常根据 M2M 应用提供者的需求强制执行，包括限制相关部署的通信模块。

除了计量数据定期报告，电子智能计量（见图 3-3）通常需要 M2M 服务器向智能计量仪发送紧急命令。当需要触发需求/响应操作时，这种情况下尤其显著，例如，暂时关闭一个设备。在这个情况下，M2M 服务器通常会触发一个特定的 SMS 发送到智能电表，这个智能电表是服务那个目标设备的。智能电表识别这个信号并触发适当的需求/响应操作。



图 3-3　电子智能计量中的自动触发

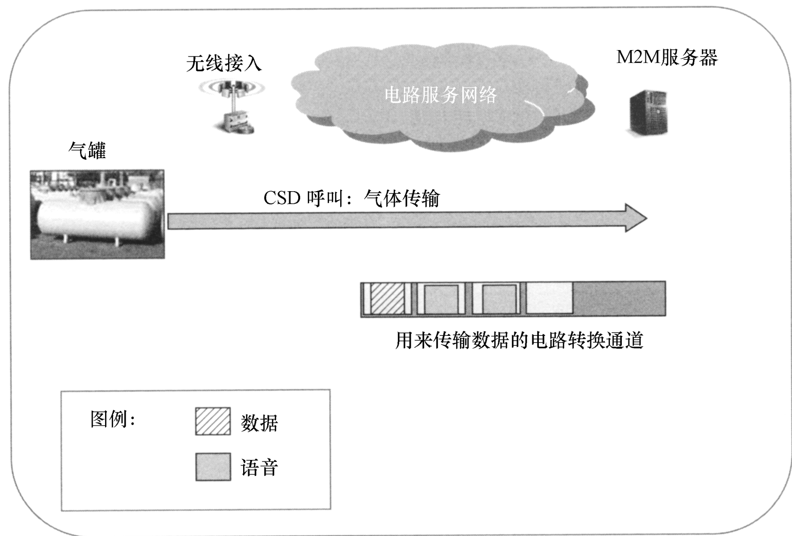


图 3-4　用于监控气罐的 CSD

另一个智能遥测的例子涉及一些能源公司使用的气罐监控（见图 3-4）。一个 MNO 网络的使用允许增加工人的安全，以及高度的运营效率。气罐的实时监测是用基于 SIM 的通信模块远程执行的，这个模块是安装在气罐计量仪中。在这个部署场景中，利用 CSD，液位被发送到中央的应用，当需要时触发适当的操作行为。

虽然 CSD 可能被读者认为是过时的，但是它的选择通常被终端用户强制执行，他们通常更喜欢避免主要现有软件的重建或昂贵的有 GPRS 功能的通信模块的集成。

3.2.2.3 医疗保健监控

M2M 电子健康应用，如远程病人监护、独居老人监护、个人健康，或疾病管理构成了主要 M2M 市场部分。本节讨论了针对西方国家老龄化人口的老龄健康应用。这个服务通常利用 M2M 设备，它被集成在一个可戴的手镯或一条项链内。它允许病人通过按 M2M 设备上的一个按钮联系急救中心。M2M 服务器识别到呼叫号码（没有应答）和自动向病人的 M2M 设备启动一个呼叫。病人然后得到一个急救医务人员（EMT）的帮助。这个过程已经实现，以确保为 M2M 服务器执行所有的计费（和相关的账单）。

此外，在这个部署场景中，另一个 M2M 服务器（一个维修中心）偶尔使用 CSD 服务来执行软件和固件升级。两个场景如图 3-5 所示，图中显示了两种行为模式。

- M2M 设备行为模式 1：收到一个呼叫时（仍就无应答），急救中心向 M2M 设备发出一个高优先级的呼叫，使用高优先级移动台国际用户目录编号（MSISDN）与 EMT 建立一个通信，这些设备已经被赋予了两种 MSISDN，那就是，一个用于高优先级服务，另一个用于所有其他服务。在这种行为模式中，人工监督对 MNO 构成了关键和高优先级的服务。使用一个特定的 MSISDN 可以允许相关的呼叫被视为一个高优先级。
- M2M 设备行为模式 2：由于 M2M 设备需要定期升级软件/固件，所以 CSD 是用第二个 MSISDN，允许网络把这种维护作为低优先级。

在早期的 M2M 部署中，根据情况的紧迫性，M2M 设备被分配两个 MSISDN 来允许网络行为的多种形式：

- 如果需要迫切建立一个通信承载，第一个 MSISDN 被用来发出一个高优先级的呼叫或得到一个高优先级的呼叫回应。该网络将使用这样一个MSISDN 确保高优先级呼叫得到高优先级的处理。其他 MSISDN 的使用是为了确保一个高优先级的呼叫使用一个空闲的 MSISDN，而它不是被用于低优先级的 CSD 通信。
- 第二个 MSISDN 被用于以一个低优先级处理的 CSD 通信。

然而，主要的缺点是潜在的 MSISDN 资源消耗的增加。因为目前还缺乏足够的

资源，如 MSISDN，所以对于未来 M2M 的部署，开发一个标准解决方案去避免对多个 MSISDN 的需求是至关重要的。

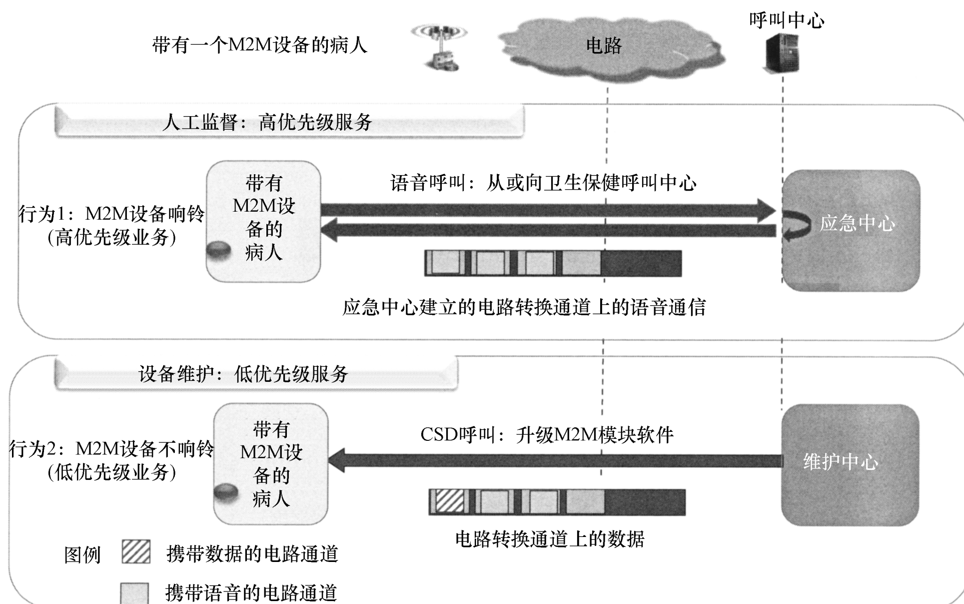


图 3-5　远程医疗

3.2.2.4　监测和安全

监测和安全的 M2M 设备部署在住宅和商业场所，比如学校、公共大楼、商店，为安全警报应用提供数据、照片和视频监控信息。蜂窝网络通常被用来作为主要的或备份入口去连接安全监控应用或房屋所有者。

交换信息主要包括报警信息和偶尔的低到中分辨率的视频信号。

当视频或照片文件需要传播时，监测和安全应用要求非常低的延迟和偶尔的高带宽。这样一个要求突出强调了使用 PS 承载的重要性。为了避免有关 PDP 环境建立中大规模的延迟，要维持一个拥有永久分配 IP 地址的不间断连接。此外，监测和安全应用还强加了其他要求，如：

• M2M 设备的认证是使用 RADIUS 协议由 M2M 应用服务器提供的（除了 MNO 身份验证机制）。这种身份验证对于 M2M 设备建立 PDP 环境是一个先决条件。

• M2M 设备的 IP 地址是从相同的子网由 M2M 应用服务器（或一个实体代表）分配的。这样的一个机制避免了使用公共 IP 地址的需要，方便不间断承载。

• 为了保护 M2M 设备的认证，以及确保 MNO 和 M2M 应用服务器之间交换数据的隐私，在 MNO 和该公司的网络之间建立了一条加密的 IP 安全性（IPSec）通道，其中 M2M 应用服务器被托管。

图 3-6 提供了一个用于监测和安全应用的网络装置的说明。

步骤 1 ~5 说明 PDP 环境的建立。在身份验证成功之后，M2M 设备使用 RADIUS 协议被分配一个 IP 地址。如果破坏或违反（步骤6），M2M 设备自动从安装在建筑物里的摄像头收集证据（步骤7）（照片或视频）。在步骤8 中，利用预先建立 IPSec 通道（步骤0），证据通过不间断 PDP 环境在 TCP/IP 连接上传输，而不需要建立一个网络承载。操作员可以在向房屋发送一组证据之前执行最初的检查。操作员可以发出一个呼叫到终端用户，并用图片或视频反馈验证故意的破坏（步骤9）。

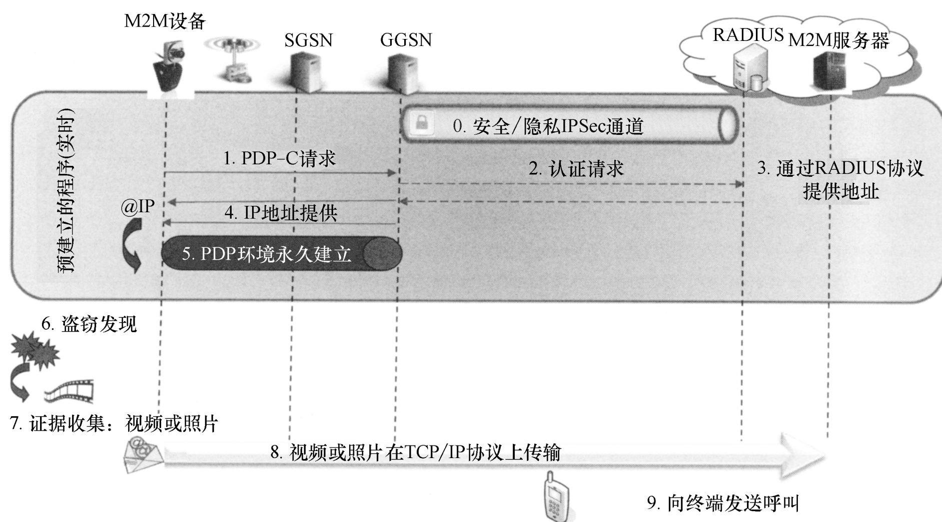


图 3-6 不间断保护和远程监测

3.2.2.5 销售点和自动取款机

为了管理金融事务和现金分配过程，销售点（PoS）和自动取款机（ATM）被广泛部署。通常，PoS/ATM 终端设备都配备了广域网连接（无线或有线）以允许与中心服务器通信，以便管理付款/现金分配交易。除了对交换数据强大的安全性和完整性的需求，PoS/ATM 应用面对的主要挑战之一是能够提供近实时的服务，依据与终端用户高度的互动性它被强制执行。这样，通过使用不间断连接解决了这个需要，避免了由 MNO 建立一个 PDP 环境而引起的过度延迟。

图 3-7 描述了一个电子支付的部署。步骤 0 ~5 说明了 PDP 环境的建立。在使用 IPSec 通道成功验证身份之后，M2M 设备被分配一个 IP 地址。

一旦客户来付账，终端按照支付事务的要求与 M2M 服务器执行数据交换（步骤 6 和 7）。

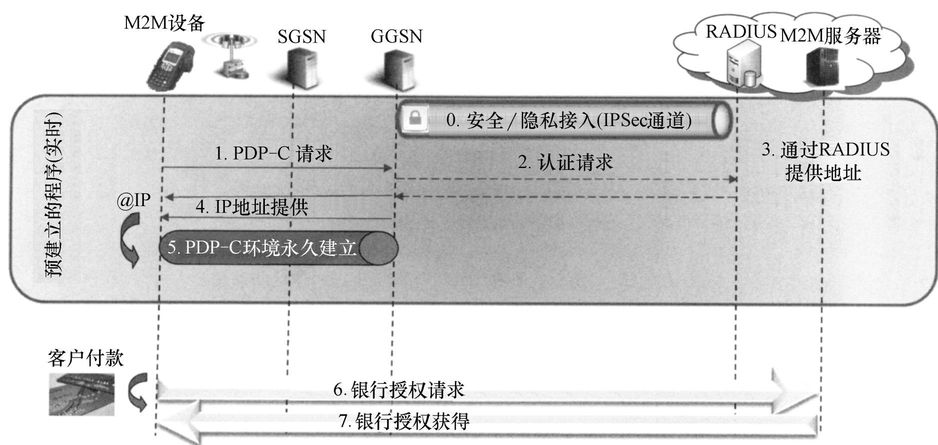


图 3-7　不间断电子付款说明

3.2.2.6　从早期 M2M 例子得出的一般结论

一个可以从早期运行部署中得出的结论是解决方案的选择本质上依赖目标应用需求的特性。一般来说，下面的应用需求必须被考虑：

- 端对端延迟和互操作性要求；
- 数据量；
- 数据交换频率；
- 服务器与客户端的初始通信；
- 通信模块功能。

根据应用的需要，表 3-1 提供了一个使用网络解决方案的总结。虽然表 3-1 提供了通用的规则，但是最后的决定常常不得不连同已安装的旧应用和通信模块一起考虑其他约束，如终端用户的需求。

表 3-1　M2M 解决办法和用例例子映射

用例需要	CS 域/PS 域	连接模式	描述	赞成者	反对者
实时/交互数据	PS 域	一直打开	M2M 设备有一个永久激活的 PDP 环境，允许一直连接	没有关于数据承载建立的延迟	环境为每个承载维持在网络设备中（额外的 CAPEX 和 OPEX 成本）

（续）

用例需要	CS 域/PS 域	连接模式	描 述	赞成者	反对者
中到高的数据量（但无实时要求）	PS 域	为数据转移周期建立的 PDP 环境	当通信由服务器发起时，设备触发是服务器主动执行的，向 M2M 设备发起一个 SMS 或无应答的呼叫来请求 PDP 环境的建立。或者，M2M 设备建立 PDP 环境，例如有数据要报告时	避免了为每个 PDP 环境在一个永久基础上维持环境的需要	尽管实际数据交换是在 PS 域上执行，但 CS 域仍然在被使用
低的数据量和周期性	CS 域	语音或 SMS	语音电话/SMS 产生短信息传播	没有 PS 域信令的昂贵的使用；仅仅是少量的数据传输	CS 域资源上额外的开销
高级可用性数据服务	CS 域	有多个 MSISDN 的数据 CSD	CSD 呼叫产生一个专门的 MSISDN	高优先级的呼叫用高优先级路由	需要两个 MSISDN

3.2.3 早期 M2M 部署常见问题

本节介绍了一个对一些[1]早期 M2M 部署遇到的问题的概述。在确保大规模主流 M2M 部署中，通过适当的网络设置，并通过新的目前被定义在标准中的特性解决这些问题，是一个成功的关键因素。

3.2.3.1 阻塞和过载

作为一个对可能发生拥堵的地方的说明，图 3-8 表明了可能遭受拥塞和过载的网络设备。

通常，当 M2M 设备要求建立 PDP 环境时，拥塞问题就会发生。如果建立 PDP 环境失败，M2M 设备将保持不断的尝试，直到它们建立一个连接。

由于异常高数量的请求，身份验证服务器（RADIUS）在这个过程中开始过早的过载。当常规的人对人（H2H）PDP 连接请求来到数据包核心网络时，身份验证服务器无法回复和发回一个超时失败的响应。过载通过网关 GPRS 支持节点（GGSN）接口传回，结果在后来的阶段冻结了整个数据包核心网络。

网络管理员往往需要暂时停止 M2M 业务，作为一种来确定和隔离错误或故障

[1] 记录所有部署中遇到的问题可以自成一章。

通信模块的手段。然而，由于同样缺乏手段去识别特定的 M2M 业务，这样的一个操作可能也不容易实现。

相对于通常在电信网络基础设施上传输的 H2H 业务，依据一个对 M2M 业务行为的初步分析，可以推断出以下特点：

● 同步性：M2M 设备通常被规定在给定时间间隔内报告数据，比如每小时，在连接的建立中没有任何随机。依据网络资源的使用，这种行为将导致同步，也经常导致堵塞。

● 不可预测性：在其他情况下，在操作员没有意识到这样一个部署符合于 M2M 的情况下，M2M 模块就被部署。在这种情况下，对操作员来说，预测相应网络的通信量和规格会变得困难。

● 突发性：一些设备，如监测和安全设备，通常产生少量的数据，除了当已经出现一个报警时。例如，当有一个报警时，一个摄像机可以产生很高容量的数据。

● 无法控制性：一组设备随机地连接到网络，没有任何可预测的模式。例如，一组漫游设备，当它们失去操作员 A 的覆盖（由于无线电问题），同时它们将会尝试漫游到操作员 B。

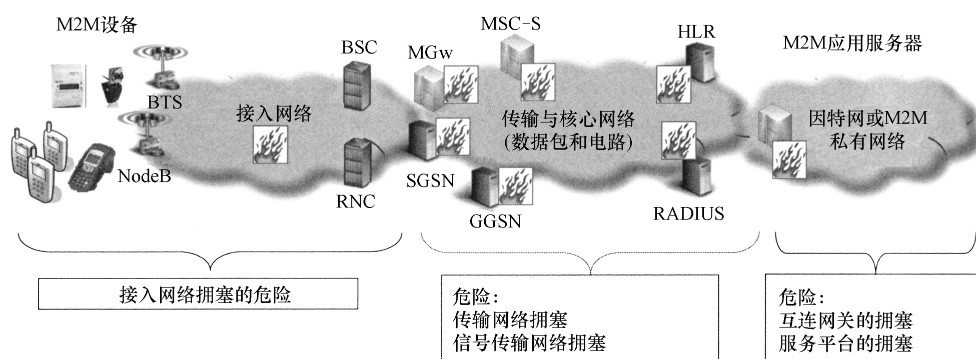


图 3-8　M2M 设备中的拥塞

3.2.3.2　识别和寻址资源的短缺

MSISDN 用于识别移动终端。它们还提供一个人性化的方式来达到一个特定用户终端。在当前 MNO 部署中，无论它们是为了 M2M 或其他人工通信，每个用户都被分配一个 MSISDN。MSISDN 格式在 ITU-T 的推荐 E.164 中被详细说明。虽然它允许大量的设备部署，在不同的国家，国家编号计划已经把可能的数量限制到很小的数字（根据对个人通信的预测）。让我们举例来说，例如法国，以下的街区编号被分配给移动运营商：06 XX XX XX XX 和 07 XX XX XX XX。这样的编号计划允许最大值 2 亿的用户，这对一个人口为 6500 万的居民是足够的，一旦 M2M 已经被大规模部署，也可能达到其极限。在早期的部署阶段，一个优化这些资源的替代

方案是使用私有 MSISDN 计划。不幸的是，这个解决方案具有一定的局限性，如漫游时服务的互操作性。因此，这种方法可能对国外旅行的连接汽车不起作用，它必须能够为了继续提供服务而漫游。

- 当 M2M 设备建立数据承载时，IP 寻址被使用。根据不同的部署场景和需求，公共和私有的 IP 寻址都是可用的。为了优化 MNO IP 寻址资源，私有 IP 寻址可被使用，但需要一个特定的网络设置，既能为一个 M2M 服务器和它控制的 M2M 设备建立特定的私有网络，又能在 M2M 服务器位于互联网时部署一个网络地址转换器（NAT）。私有 IP 寻址具有以下限制。
  - 关于 NAT 部署额外的成本；
  - 对于服务器发起通信，M2M 服务器可能无法达到 M2M 设备，除非部署明显的机制去打开 NAT 中的漏洞。因此，即使 M2M 设备有一个已建立的 PDP 环境，它仍然需要通过 SMS 触发设备。

3.2.3.3 为了纯数据服务使用 CS 域环境

虽然有人可能争论一个仅使用 PS 域服务配置的 M2M 设备可能不需要有一个 MSISDN，但是实际上，因为其中一些程序，3GPP 标准仍然要求需要一个 MSISDN，比如计费，依靠使用一个 MSISDN 来作为标识符。此外，使用 SMS 作为一个设备的触发机制需要一个 MSISDN，以及对 CS 域订阅，还有对 PS 域的订阅。由于需要维护一个 CS 域便签中的环境，这样一个对 CS 域的订阅是有一定成本的。

当前 SMS 的 3GPP 标准使用 MSISDN 发送一个 SMS。正在进行中的 3GPP 工作都是通过允许只有 PS 订阅和发送 SMS 到一个国际移动用户识别码（IMSI）来向减轻这种约束发展，这不需要一个 MSISDN。

3.2.3.4 早期部署问题的总结

虽然有几个与早期 M2M 部署相关的问题，但迄今为止最重要是关于过载和拥塞的问题，以及稀有编号和寻址资源的缺乏。对于这两个问题，标准和监管机构正在努力提供长久的解决办法，允许 M2M 中无缝且具有成本效益的增长。对于寻址而言，尽管目前 IPv6 的发展势头对于可预知的未来能提供具体的答案，但是它的大规模部署经常遇到终端用户部署的障碍。

至于拥塞和过载控制而言，这变得非常明显，那就是虽然标准发展应提供长久的解决办法，但在短期内就需要一个解决方案来允许目前 M2M 部署的增长而不影响网络的稳定性。这种解决方案的要素将在下一节中提供。

3.2.4 M2M 部署可能的优化

本节概述了目前在网络规划和结构允许 M2M 部署增长方面的最佳实践，而新标准也正在开发来允许一个长期的解决方案。在本节的其余部分中，介绍了业务量识别。业务量识别是允许为 M2M 建立优化架构的一个基本功能。

3.2.4.1　业务量识别

识别 M2M 业务量本身就是一个基本的推动者，为了：

- 优化运营网络来更好地处理 M2M。在本节的其余部分，演示了特定的核心网络设备如何可以为 M2M 订阅而专用和优化。
- 提供 M2M 具体的运营管理和维护（OA&M）功能。例如，由于一组有故障的设备而发生的拥塞，通常完全禁用这套造成拥堵的设备是令人满意的，例如，与 M2M 服务“ABC”有关的 M2M 设备。二者选其一，相关的订阅可以被路由到另一个网络设备，以免影响敏感的服务。这样做，网络管理员有办法阻止附带损害和操作维护其他服务。一旦问题的根源得到解决——例如，一个新的 M2M 设备固件版本将导致频繁的向网络连接——业务量也能在网络上恢复。

3.2.4.2　IMSI 范围的使用

业务量识别可以基于专用 IMSI 范围的使用来被执行。这些专用的范围将通过使用类别来组织，在归属位置寄存器（HLR）/归属用户服务器（HSS）和 GSM 移动业务交换中心（GMSC）上实现，来为 M2M 业务定义一个专用的路由。这个 IMSI 由 15 位数组成：前五位数被用做移动国家代码和移动网络代码；接下来的两位可以用来为 M2M 路由到一个特定的 HLR，而剩下的几位数字可以用来鉴定一个特定的终端用户，例如，实体 ABC 或某种 M2M 市场部分，例如，电子健康。

3.2.4.3　专用的核心网络中心设备

为了以无缝方式管理 M2M 用例，已经表明了识别 M2M 业务量的重要性。这一段提倡使用一个网络体系结构，其中特定网络设备致力于 M2M 业务。这些被称为“专用 M2M 链”。

图 3-9 显示了两个有专用 M2M 链的核心网络设备，它由以下部分组成：

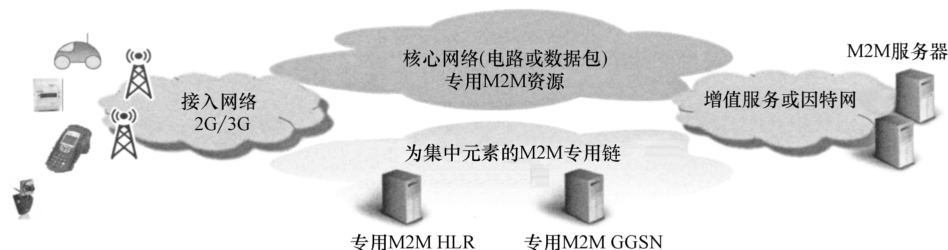


图 3-9　M2M 优化的网络结构

- HLR - 这是管理所有向网络订阅的中央数据库。M2M 特定 IMSI 范围的使用允许所有网络注册请求被路由到这个特殊的 HLR。这样做，网络运营商可以避免由大量 M2M 设备同一时间在网络中注册引起的阻塞和过载，例如，失去操作员 A 覆盖的漫游设备要与操作员 B 漫游，此外，通过分配一个特定的 HLR 到 M2M，可

以为 M2M 优化其设计和维护。例如，HLR 中为 M2M 订阅的存储空间可以通过利用这样一个事实被优化，那就是，大量的订阅信息与适合某一设备类别的订阅是共同的。同时，由于几个 M2M 设备是固定的，通过减少移动管理程序的频率可以优化 HLR，从而允许高容量 HLR 设备。

- GGSN - 除了其他事情之外，这是向基于 IP 的网络提供网关功能的网络设备，即公司或互联网，通常 M2M 服务器位于其中。设备的设计可以完全为 M2M 自定义。例如，在已经有的案例中，M2M 应用需要使用稳固的承载，但要产生很少的业务量。在这个例子中，GGSN 可以被定制和设计用较小的数据传输内存去处理无限大数量的 PDP 环境。

3.2.4.4 核心网络元素的特定设置：GGSN APN-M2M 特定配置

除了为核心网络使用专用的 M2M 链，核心网络的特定配置和优化可以进一步确保处理 M2M 的效率。本节提供了一个 M2M GGSN 接入点名称（APN）配置的示例。这样一个特定 APN 配置允许 M2M 业务精细的处理。作为一个例子，因为需要允许低的延迟和波动，一个人可以为电子健康业务选择使用一个特定的 APN。这样的一个需要将被翻译成适当的标记数据包和符合这样业务的更高优先级。

APN 是一个 GPRS 的参数，允许特定的业务路由到 IP 网络。HLR 中每个订阅都可以被指定一个特定的 APN，它在 PDP 环境的建立之上被激活。

APN 可以配置几个参数以便允许一个特定形式的行为，它通常基于一个与终端用户的共同协议：

- 连接模式可以是永久性的和非永久性的。当连接模式是非永久性的，GGSN 可以被配置在特定的超时之后释放 PDP 环境。
- IP 寻址可以被配置去使用公共或私有的 IP 地址。

表 3-2 APN 分类和建立

连接模式	IP 地址计划	APN 的名称	会话超时的 APN 计时器
一直打开	私有 公开	M2M_Al_On-Private. com M2M_Al_On-Public. com	关闭
非永久性的	私有 公开	M2M_Non_Perm-Private. com M2M_Non_Perm-Public. com	每天

- 会话超时的 APN 计时器显示一个超时之后，PDP 环境由网络释放。这种机制被用来避免维护不再使用的承载环境的需要。

在表 3-2 中，通过说明各种可能分类的形式，创建了四种 APN，它分成不间断连接或非永久性，既有私有的也有公共的 IP 地址计划。APN 的参数可以根据它们处理的业务量配置：举个例子，私有 APN“M2M_Al_On-Private.com”和

"M2M_Non_Perm-Private.com"通过 NAT 路由器路由，而公共 APN"M2M_Al_On-Public.com"和"M2M_Non_Perm-Public.com"直接通过因特网路由。用这个 APN 分类方法，M2M 业务不仅可以通过使用专用 M2M 链分开，而且可以根据客户/市场部分需要分配不同的优先级/业务处理机制。

3.3　本章小结

虽然 M2M 应用在运营网络中，但是不要简单地还把 M2M 视为其他个人通信业务，这是必要的。网络运营商，特别是 MNO 正在倡导一个两步骤的方法：

- 步骤 1 主要在于优化目前为 M2M 部署的网络。这些优化考虑了一些 M2M 的基本特征，如同步性、突发性和固定设备。一组目前最佳的实践正在周围逐步构建：
  - **专用 M2M 链**：包括为 M2M 处理分配特定的网络元素。这些元素是根据 M2M 业务需求度量的，而不是适合个人通信的常规度量。
  - **业务量识别**：包括通过使用特定的 IMSI 范围和专用 APN 为 CS 域和 PS 域识别 M2M 业务。
  - **网络设备优化**：包括为 M2M 优化特定设备。在本章中提供的示例是一个优化 HLR 的使用，例如，每个订阅中使用较小的环境和为了固定的 M2M 设备而触发不频繁移动的管理程序。

步骤 1 下的优化列表还可以继续。本章不提供所有它们的概述，这些能够从一个运营商变化到另一个，而这很大程度上取决于目标 M2M 应用。

- 步骤 2 包括基于引入彻底为 M2M 设计的新特性，提供一个长期部署 MNO 网络的修复。3GPP TR 23.888[1]为这些优化提供了一个初始起点。这些有望在将来为大规模和更加成本优化的 M2M 部署铺平道路，通过软件升级或所需新设备的部署这是可操作的。有用的网络优化的例子包括：
  - 仅 PS 订阅/无 MSISDN：这个特性对 MNO 来说不需要在 CS 域维持一个订阅环境，或者为只使用数据服务的 M2M 设备分配一个 MSISDN。
  - 在线设备触发：包括提供有效的机制来触发数据承载建立。

参 考 文 献

1. 3GPP TR 23.888 (2011). System Improvements for Machine Type Communications.

第 2 部分

M2M 的架构及协议

第 4 章　M2M 的需求及高层架构原则

Omar Elloumi，Franck Scholler
阿尔卡特朗讯公司，维利兹，法国

4.1　引言

本书的主要目的是推动 M2M 的发展。为了充分理解目前发生在不同标准的工作背后的动机，以及最近的市场开发，熟悉基本 M2M 需求是必要的。大多数标准化组织，包括 3GPP、3GPP2 和 ETSI，都采取了用例驱动的方法作为一种手段来获得进一步定义业务架构的需求。然而，ETSI 采取了一种更为正式的描述用例的方式。除了用例驱动的方法，这变得非常明显，那就是所有网络优化问题，包括设备的特点和设计或运营网络，还都必须考虑到 M2M 的基本特征——生成的业务量和增长模式。这两个问题对接入和核心网络提出了新的，特别有挑战性的需要。

虽然本章主要集中在 M2M 对业务和网络方面的要求上，但是我们的目标不是要提供一个详尽的、可以在不同的 ETSI、3GPP 和 3GPP2 标准中找到的需求清单。目的是为了展示这些要求是怎样得出的，以及 M2M 给潜在的系统强加了哪些新约束。在 M2M 通信中关于 IP 角色的需要在第 7 章中进行了更详细的描述。

下一节将主要集中在 ETSI M2M 用例和 M2M 业务层的需求。

4.2　用例驱动的方法实现 M2M 需求

4.2.1　何谓用例

用例这个术语是很常用的。然而，很难找到一个公认的定义。对象管理组织（OMG）提供了一个优秀的描述用例的定义和方法。根据 OMG，一个用例一方面描述了一个或多个参与者之间的交互，另一方面是正在考虑中的系统之间的交互。这些交互被表示为一系列简单的步骤。参与者是存在于系统之外的某物（一个终端）或某人（一个人或一群人）。参与者参加一系列与系统的交互来实现一个给定的目标。

用例把系统视为一个黑盒子，在它里面来自系统外部与系统的交互，包括响应，被感知。一个用例将被以一个架构中立的方式描述，这种方式不采用任何特定

的物理架构。

用例不应与正在考虑中的系统的功能、特点，或要求混淆。一个用例可能与一个或多个功能和/或需求有关。一个功能或要求也可能与一个或多个用例有关。

一个用例还将描述这个参与者通过与系统的互动要完成什么，这个是目标。

4.2.2　ETSI M2M 的用例

ETSI 的 M2M 技术委员会（TC）成立于2009 年1 月，旨在提供一个 M2M 通信架构的端对端视图。这个端对端视图并不意味着 M2M 系统的所有元素都被 ETSI TC M2M 指定。这项工作完全支持发生在其他标准化开发组织（SDO）和论坛中优先使用了最先进技术的工作和正在进行的标准化的努力。TC M2M 主要聚焦于业务层方面，在适当的情况，是指其他标准活动。ETSI TC M2M 做了一个慎重的决定，那就是以用例中的一组应用实例的工作为基础，其中用例构成了向所需定义的输入。

ETSI 决定以其用例驱动方法为基础，这个方法中有五个主要用例成员：

- 智能计量；
- 电子健康；
- 联网消费者；
- 汽车；
- 城市自动化。

ETSI 已经开发出了五个技术报告来获得这五个用例成员。根据这些技术报告，目前 ETSI TC M2M 正在开发一组规范。图 4-1 描述了用例技术报告和其他可交付成果之间的关系。

在用例上的工作并非面面俱到，因为一个系统的方法可能会变得很麻烦和耗时，并没有真正提供多大的额外价值。此外，记录所有潜在的用例可能为参与者之间的创新和区分留下很小的空间。目标是能够覆盖足够的用例，以确保所有重要需求能被满足，以便架构工作为潜在的大量 M2M 应用提供基础。

4.2.3　用例开发的方法论

由于多种可能的用例，用一个单一的方法来开发用例是这个过程中的一个必要步骤，这已经变得越来越清楚。

4.2.3.1　用例模板

为了允许以一个最小的形式描述用例，当获得需求时，使用单个模板是实现共同的理解和某一形式的基础。

下面的模板，与来自参考文献［1］中的一样，已经被 ETSI TC M2M 使用：

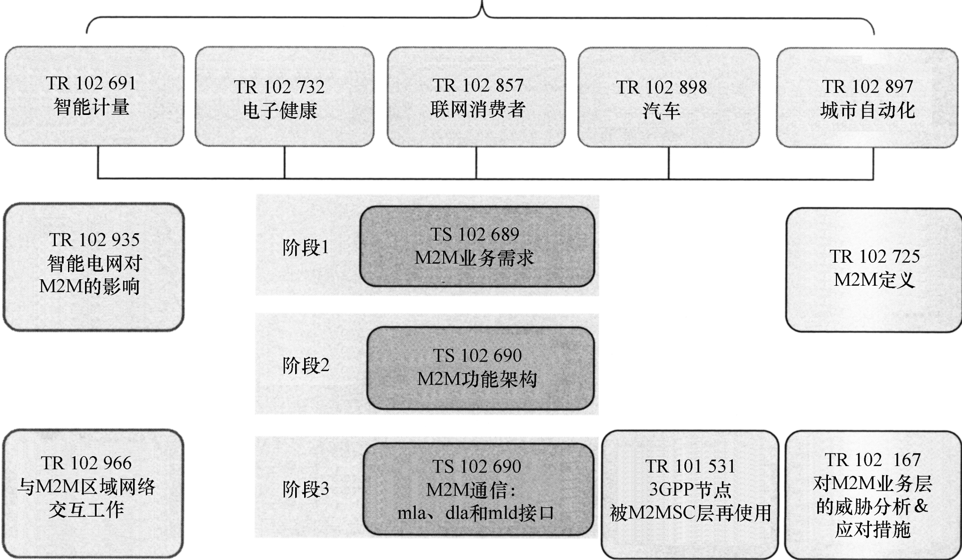


图 4-1　ETSI TC M2M 方法，对业务需求的用例驱动方法

模板

一般用例描述

在高层术语中用例的对象/目标列出了主要突出的问题。

利益相关者

用例指的是谁或是什么的列表：消费者、网络运营商、数据库、账单实体等。

场景案例描述

用例的描述性文本展示了利益相关者是如何使用这个系统的。这部分可以为用例提供前提条件以及触发。

信息交换

信息流的逐步描述，例如注册、数据检索，或用例暗含的数据发送。

潜在的新需求

来源于用例的需求列表。

用例源

参考文档或开发用例的实体。

4.3　ETSI M2M 智能计量方法

4.3.1　引言

按照一项单独 ETSI M2M 技术报告[1]，智能计量用例在 ETSI M2M 中被使用。

这项工作与欧盟委员会关于智能计量的 M/441 授权密切相关，并由它驱动。授权 M/441 具有以下目标：

这一授权的总目标是创建欧洲标准，将使公用事业计量表（水、气、电、热）的互操作成为可能，它可以改进这种方法，通过这种方法客户实际消费水平的意识能得到提高，以便及时适应他们的需求（通常被称为“智能计量”）。

智能计量主要把提高能源效率作为目标，因此主要为了促进能源消耗的减少，以及减轻二氧化碳和其他温室气体的排放。

智能计量设备是公用事业计量表（水、电、气、热），消除了估算账单和人工仪表读数的需要，并提供给客户、能源分销商和供应商准确及时的关于可消耗实体（如电力、天然气）使用情况的信息。智能计量设备还可以提供其他服务，比如实时能源消耗控制的能力。

智能计量协调小组（SMCG）——一个 CEN、CENELEC 和 ETSI 的联合小组，主要为在智能计量领域协调标准化活动——它的一份报告[2]记载了一组功能，它们被建议由智能计量信息系统提供。这个列表分成六个类别，代表了在通常由传统计量表提供的那些功能之上提出的额外功能。六个类别的功能如下所述[1]：

- 计量寄存器的远程读取和对指定的市场组织的规定：计量系统的功能是通过一个在预定义的时间计划中的或根据要求的标准接口给指定的市场组织远程提供计量表寄存器的值。
- 计量系统和指定市场组织之间的双向通信：计量系统的能力是去远程检索数据，例如，使用、网络和供应质量、事件、网络或计量表状态，以及非计量数据，使这些数据对指定的市场组织是可用的。指定市场组织的能力是远程配置计量系统和执行固件/软件升级。计量系统接收信息的能力，例如，信息从能源服务提供商（和/或通过相关的第三方，例如，分配系统操作员或计量运营商）发送到终端用户的客户。
- 支持先进收费和支付系统的计量表：计量系统的能力是允许客户以适当的付款方式为使用预付款，在预定的消费或一定的持续时间后连接到一个电源和断开它。支持收费：计量系统为消费提供多率寄存器，（在适用情况下）注入允许，例如，对于使用收费的时间、临界的峰值、实时定价或这些的组合。
- 允许供应远程禁用和启用的计量表：计量系统的功能是远程允许指定的市场组织安全控制或配置供应限额（不适用于燃气表），通过计量表上可配置的参数设置启用和禁用供应。
- 为了显示和潜在的分析，安全通信启用智能电表给终端用户或被终端用户指定的第三方输出计量数据。
- 通过入口/网关提供信息给室内/建筑显示器或辅助设备的计量表：计量系统的能力是为外部视频显示器提供总使用量的信息以及其他计量的和非计量的数据。

在用例开发期间，“附加功能”已经为了用例的开发被用来作为一个通用的框架/范围。这样，每个用例都被附加上一个或多个功能。

4.3.2 典型的智能计量部署方案

图4-2提供了一个典型的智能计量系统的设备部署方案。这个方案展示了智能计量设备（例如，阀门，电表，燃气表，水表）通过通信网关被连接到数据中心。

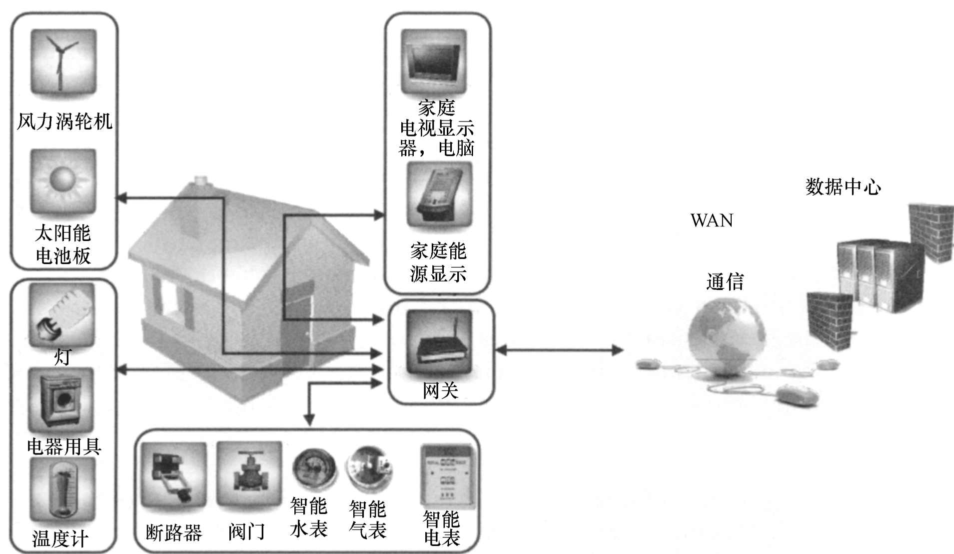


图4-2 智能计量系统的典型部署方案，ETSI允许复制

数据中心从智能计量设备收集数据，并能够通过通信网关远程控制相关的智能计量设备。

在这个方案中，网关向家庭自动化设备，如传感器（如温度传感器）、显示器和家用电器，还有在居住环境中部署的电力微发电机提供一个接口。

智能计量用例的例子：预付款功能。这个用例是来自于参考文献［1］。

一般用例描述

配置一个智能计量信息系统是为了支持预付款功能，与被计费实体定义的一样。用例描述的场合是预付款功能在智能计量信息系统上被本地管理以及管理被计费实体远程执行的情况。

利益相关者

计费实体

负责给消费者开账单的组织。

消费者

消费电力、天然气、热或水为前提的组织或个人。消费者也可以是与计费实体签订合同来付费的组织或个人。

资产实体

负责智能计量信息系统资产（例如，计量通信设备，智能计量网关）安装、配置、操作和维修的组织。

场景案例描述

先决条件：智能计量表系统被安装和配置来作为一个预付系统。智能计量信息系统识别计费实体和/或资产实体，给它们一个地址。

后置条件：智能计量信息系统确认预付触发操作已经完成的计费实体和/或资产实体。

计费实体和/或资产实体能意识到故障的发生。

触发：付费实体或消费者决定需要在智能计量信息系统上执行一个预付款行为。

信息交换

基本流程

1. 资产实体或计费实体发送一条消息到智能计量信息系统来改变付款方式。
2. 智能计量信息系统验证请求。
3. 智能计量信息系统改变付款方式。
4. 资产实体或计费实体收到付款方式更改完成的确认。
5. 智能计量信息系统从资产实体和/或计费实体显示预配置信息。
6. 消费者通过一个显示器读取这些信息。
7. 消费者能够按照这一信息行事。
8. 消费者根据这个信息采取一个行动，例如它向智能计量信息系统增加信用或减少紧急信用安排。
9. 当动作完成时，智能计量信息系统向资产实体和/或计费实体发回确认消息。
10. 智能计量信息系统按预定时间间隔或者根据来自计费实体的要求提供状态信息。

可选流程 1

步骤 2 失败：智能计量信息系统无法验证一个请求：

1. 资产实体或计费实体发送一条消息到智能计量信息系统来改变付款方式。
2. 智能计量信息系统认为请求无效，无法改变付款方式或显示预配置的信息。
3. 智能计量信息系统连同日期/时间标示一起记录事件（错误）。

4. 智能计量信息系统通知资产实体和/或计费实体发生了一个错误。

5. 结束。

(…)

可选流程 3

步骤 5 失败：智能计量信息系统未能显示来自资产实体和/或计费实体的预配置信息：

1. 资产实体或计费实体发送一条消息到智能计量信息系统来改变付款方式。
2. 智能计量信息系统验证请求。
3. 智能计量信息系统改变付款方式。
4. 资产实体或计费实体收到付款方式更改完成的确认。
5. 智能计量信息系统未能显示来自资产实体和/或计费实体的预配置信息。
6. 智能计量信息系统认为请求无效，无法显示预配置的信息。
7. 智能计量信息系统连同日期/时间标示一起记录事件（错误）。
8. 智能计量信息系统通知资产实体和/或计费实体发生了一个错误。
9. 结束。

(并不是所有的可选流程都被重述，参考文献［1］中提供了完整的列表)

来自用例的新需要：

- M2M 系统应该为 M2M 区域网络支持自动配置功能。
- M2M 系统应该支持精确的和安全的时间同步。M2M 设备和 M2M 网关可能支持时间同步或安全时间同步。
- M2M 系统应该支持远程更改 M2M 设备状态的能力，例如启用或禁用。
- M2M 系统应该支持能够处理此功能的合作对象之间事务处理。
- M2M 系统应该支持以下机制，用于接收来自 M2M 设备和 M2M 网关的信息：
  - 接收未经请求的信息（被动检索）。
  - 接收预定信息。
- M2M 系统的末端应该可以验证交换数据的完整性。

用例源

ESMIG（欧洲智能计量产业集团），文件：智能计量功能的用例，ESMCR003-002-1.0，2009 年 10 月。

这种智能计量的用例由欧洲工业协会、ESMIG 提供，以满足 M2M 系统提出的几个要求。举个例子，支持事务的需要。用例清楚地表明，所有预付流程的步骤是不可分割的，在某种意义上，该业务只有当所有预期的动作已经正确执行时才有效。如果不是这种情况，那么要强制回到原始状态。事务被定义为一组不可分割的操作（即像原子一样密不可分），也就是说，如果一个操作失败，那么其他操作的

结果必须取消。事务管理代表了一个对 M2M 系统重要的要求，因为它被几个 M2M 应用所需要，有人论证，一旦这种功能可以从开发和测试中受益，然后就会为不同应用通过开放 API（应用程序编程接口）提供一种能力。

现在来考虑一个事实，智能计量表将会连接到一个通信基础设施，它既可以被一个实体拥有，也可以被网络运营商拥有。将网络连接到电表使系统易受到恶意和虚假使用的攻击，也强加了一些安全需求，如在智能计量表和后端应用或平台（代表应用）之间执行共同认证的需要，以及所有交换消息的验证。同样，应该有一个方法来验证智能计量表上运行软件的完整性，确保设备没有被篡改或其软件图像没有被恶意用户改变。另一个恶意使用的例子是当 SIM 卡被用于另一个设备时，例如，浏览因特网。

最后，智能计量表常常需要定期向后端应用报告计量数据（例如，每小时）。然而，几个用例显示了允许公用事业后端应用既要求在任何时间点发送命令（在此用例中，预付相关命令），又需要一个主动的计量读数，例如在高峰需求时期。当技术允许计量表能够不间断连接和不断接入时（例如，一个仪表通过 PLC 连接，电力线通信），公用事业后端应用触发并不要求强加特定的约束。然而，如果计量表通过蜂窝系统连接（例如 3GPP 或 3GPP2），其中典型的连接被终端㊀请求（在这种情况下，智能测量仪），这就为网络提出了一个新的需求去允许网络初始化应用连接到一个特定的终端。现在这通常通过利用特定的 SMS（触发终端建立数据连接）去做。然而，在这个特定的场景中使用 SMS 被证明是代价高昂的，因为它迫使网络运营商保持循环的订阅（只为发送 SMS 的目的而被需要），另外数据订阅用来交换应用数据。在未来，M2M 将越来越多地在网络上施加新的要求，就是允许网络初始化连接的建立，这被网络应用或一个实体所要求，其代表就是一个水平业务平台。这个特定的需求正在由 3GPP 在下列技术报告[3]中满足的，它被称为设备触发。

4.4 ETSI M2M 中的电子健康方法

4.4.1 引言

电子健康应用和相关的设备正在被越来越多地为这项应用而部署，如：

• 远程病人监控（RPM）：使医疗保健提供者通过远程收集、存储、检索、分析病人与健康有关的信息来监控和诊断健康状况。RPM 设备允许医疗保健提供者

㊀ 除了在长期演进中，默认的数据承载提供始终保持连接的方法。

在病人情况变得更加严重之前来治疗他们，从而避免了去急诊室不必要的往返和再次到医院。最后，RPM 让住院时间大大减少，从而减少相关医疗保健服务的支出。通常，一个或多个传感器被用来监控病人的生命体征，如血压。通常使用一个单独的设备（称为网关）报告监控信息，这个设备通常是连接到蜂窝网络中的。

- 疾病管理：对电子健康一个常见的 M2M 应用用法是支持病人疾病的远程管理，这一过程称为疾病管理，处理比如糖尿病或心律失常的情况。对于某些疾病管理应用，为了应对一个至关重要的健康状况，需要一个报警功能来触发一个警报去引起医生或患者的注意。
- 独居老人监护：电子健康 M2M 应用可以使老年人过一个独立的生活和留在可能经常需要帮助的家里。它由监测病人的生命体征，如脉搏、体温、体重或血压组成，确保病人服药和跟踪他们的活动水平。
- 个人健康和健康改善：电子健康 M2M 应用可以被用来记录保健和健康指标，如在锻炼期间的心脏和呼吸频率、能源消耗和脂肪燃烧率。它们还可以用于记录锻炼的频率和持续时间、锻炼的强度、跑步距离等。当这些信息被上传到一个后端服务器，它可以被用户的医生作为他们的健康状况的一部分，以及给用户的私人教练提供他们的锻炼计划进展的反馈。它让锻炼或理疗更精确、更迅速地适应病人/用户的需要。

ETSI TR 102 732[4] 提供了以下关于电子健康设备组以及网络方面的解释：

“为了获取关于一个病人保健和健康的信息，必须使用合适的传感器。因为这个原因，病人或被监护的人通常戴一个或多个传感器设备来记录保健和健康指标，如血压、体温、心率、体重等。因为这些传感器通常不得不应对有关波形系数和电池消耗的严重限制，预计在大多数情况下，它们需要通过某种形式的短程技术将收集到的数据传送到一个设备，这个设备能作为一个收集信息的整合器和一个通向后端实体的网关，这个实体被期望去存储和合理地回应收集到的数据。也有可能的是，用于监控关于病人健康状况参数的传感器就位于病人附近的某个地方。”

用于电子健康应用的传感器的例子如图 4-3 所示。当使用多个传感器时，一个网关（通常与 WAN 连接）通常被部署。网关整合和传送传感器收集的数据到一个中央应用去处理信息和在需要的时候触发相应的动作。便携式传感器通常使用短程无线接口通过 WAN 连接到网关设备，允许数据报告。虽然这样一个网关可能是一个手机或家里的一个家用网关，但是也经常使用一个带有蜂窝网络订阅的专用设备。

电子健康用例介绍的需求与其他 M2M 应用一样，都是依据注册、身份验证，以及需要终端初始化和网络初始化都进行数据交换。下面提供了一系列需求，其中电子健康提出了非常具体的要求：

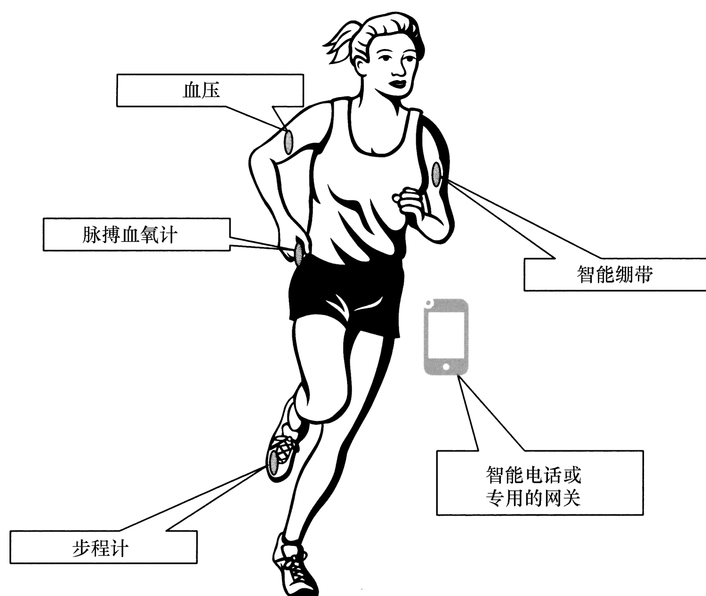


图 4-3　便携式传感器

- 位置跟踪：M2M 设备和支持系统（和应用）必须提供方法去跟踪和报告病人的位置。为了向急救医务人员（EMT）或救护车服务、附近的医院等提供位置信息，这些信息在紧急情况下可能是至关重要的。
- 支持关键时刻消息的处理和传送：一些关键警报必须及时地发送到适当的应用，特别是在紧急事件中。
- 支持时间安全同步：报告的数据必须提供准确的时间标记，因为这个精度在数据分析过程中是非常重要的。

4.4.1.1　电子健康用例的例子：干扰隔离

本节提供了另一个 ETSI TC M2M TR 102 732 中描述的用例示例。选择这个用例是因为它展示了 M2M 系统提出的非常独特的要求。

一般用例描述

在一个远程病人监控的情况中，远程健康监测的目的是为了获得低电压的身体信号，这个获得过程可以被无线电传播活动干扰，如 GSM/GPRS，这可以发生在同一 M2M 设备最近的共同协作的无线电部分。

健康监测过程被不断应用到病人，例如，发现心律失常，获得信息的活动可能被由 M2M 设备执行的典型的蜂窝无线电通信活动所干扰。

避免或减少任何可能的关于传入信号本身的干扰变得至关重要，这样可以实现一个可靠的电子健康服务，即使它不被称作是一个救生服务。

一个对付意想不到的破坏性信号传输的方法是，为了调整旨在减少干扰影响的采样信号过程，同时采样一个无线电传输指示信号，例如，通过丢弃或纠正那些收到的与活跃的无线电传输指示样品有关系的采样信号，或稍微转换信号采样的时间。另一种方式是通过在有时间限制的测量期间中断无线电传输，然后在测量时间结束时恢复它，这样去控制无线电发射机。

利益相关者

病人：病人可能是任何个人或可以使用远程监控设备（RMD）收集测量、数据或事件的代理。病人测量可以在各种临床环境，例如医院，或非临床环境，比如在家里、在办公室、在学校、在旅途，或在辅助生活设施。

RMD：一个带有传感器、用户界面和/或驱动器，以及一个 M2M 网络接口的 M2M 电子设备。该设备收集病人信息，通过 M2M 网络与适当的 M2M 服务能力提供者和/或 M2M 应用通信。一个 RMD 也可能通过一个 M2M 网关与这些实体通信。此外，该设备可以接收和/或执行来自 M2M 服务能力提供者和/或 M2M 应用的命令，或提供信息给病人。这些设备有可能需要低功耗、低复杂度协议。

M2M 服务能力提供者

一个给 M2M 应用实体提供 M2M 通信服务的网络实体。这些应用程序可以支持特定功能，帮助促进健康信息互换的行为。此外，M2M 服务能力提供者与 RMD 通信来收集数据或发送命令。

M2M 应用实体

一个被创造绑定在一起的术语，看做是一个单独的系统元素，M2M 范围之上的利益相关者。高级应用，如独立的或地理卫生信息交换、数据分析中心、综合保健服务网络，提供组织、健康记录银行，或公共卫生网络，和/或专业网络都是 M2M 应用实体的例子。术语 M2M 应用实体还包括下面典型的 RPM 利益相关者。

信息交换

用例适用于大多数电子健康应用，如 RPM。因此，信息交换的描述与源自相关需求的描述是不相关的。见参考文献［4］中的信息交换。

来自用例的新需要

- 电子医疗装置的无干扰：M2M 系统，或它的部分，应该避免扰乱低压信号的检测和测量，这样 M2M 应用才能获得和使用它。例如，在电子健康应用中，心电身体信号不断被一个无线传感器网络测量，身体网络就会被最近的属于电子医疗设备 M2M 网关的 GSM/GPRS 发射机严重破坏。
- 无线电传输活动指示：根据 M2M 业务的类型，所有 M2M 设备（或网关）的无线电传输部分（例如，GSM/GPRS）应向 M2M 设备上的应用/网关提供一个无线电传输活动的实时指示。

● 无线电传输活动控制：根据 M2M 服务的类型，所有 M2M 设备（或网关）的无线电传输部分（例如，GSM/GPRS）可能会被 M2M 设备/网关上的应用实时指示，来暂停/恢复无线电传输活动。

用例源

意大利电信公司对 M2M ETSI TC 的贡献。

该用例提供了另一套具有挑战性的需求：如果 GSM/GPRS 设备用来传送测量数据，那么它必须不被身体信号干扰，以确保测量数据的准确性。此外，当执行关键传感时，需要一个机制来允许暂停和随后恢复数据传输。

4.5　ETSI M2M 服务要求：高层概括和不同细分市场的适用性

表 4-1 提供了一个 M2M 需求的高层次总结，它被描述在 ETSI TS 102 689[5] 中。这个表并不意味着提供了一个详尽的业务需求清单。而是向读者提供了一个基本需求的概要以及不同家庭用例的映像。

表 4-1　ETSI M2M 用例对 M2M 服务业求的映射

要　求	细分市场的可应用性				
	智能计量	电子健康	汽车	联网消费者	城市自动化
通信中介					
支持不同承载技术（SMS，GPRS，和 IP）	√	√	√	√	√
向睡眠设备的消息传送（当设备在网络上变得可用时通过存储和传送）	√	√	√	√	√
通信路径的选择（根据配置策略选择合适的承载）	√	√	√	√	√
通过网关与设备通信	√	√	√	√	√
通信失败通知	√	√	√	√	√
信息传送确认	√	√	√	√	√
精确、安全的时间同步和时间采样	√	√	√	—	—
位置支持					
向 M2M 应用报告 M2M 设备/网关位置	—	√	√	√	√
加强有关位置的隐私性	—	√	√	√	—
数据收集和报告					
周期性报告	√	√	—	—	√

（续）

要 求	细分市场的可应用性				
	智能计量	电子健康	汽车	联网消费者	城市自动化
按需报告	√	√	√	√	√
基于事件的报告	—	√	√	√	√
使用由基础网络提供的 QoS	—	√	√	√	√
路径差异（主路径和备份路径）	—	√	—	—	√
M2M 设备与多种终端应用相互作用	√	√	√	√	√
安全					
通信实体之间的相互认证	√	√	√	√	√
数据转移的机密性（加密）	√	√	√	—	√
数据转移的完整确认（交换数据的认证）	√	—	—	√	—
避免一个 M2M 通信模块用于一般的通信目的	√	√	√	—	√
设备/网关完整性验证	√	√	—	—	—
安全证书和在应用层的软件升级	√	√	√	√	√
命名和寻址					
设备名称而不是网络地址被应用程序使用	√	√	√	√	√
支持多种地址计划，例如 IP、E.164 等	√	√	√		√
远程管理					
故障管理（主动监视、故障发现、连接认证、故障修复等）	√	√	√	√	√
配置管理（网络的配置和服务参数，新应用版本安装）	√	√	√	√	√
软件升级、固件升级和补丁	√	√	√	√	√

最重要的结论是，从表中可以得到几个 M2M 应用也有类似的需求，它们可以通过使用稳定和经过良好测试的软件模块被处理，从而使一个用例有一个更简化（更轻量级）的应用和开放 API 揭示 M2M 服务功能的需要。

进一步的结论是，与个人通信相比 M2M 强加了新的业务需求。例如，考虑智能电表的例子。公用事业提供商期望这些设备项目要被部署至少 20 年。这么长的部署阶段要求在设备项目的生命周期里需要去升级安全算法和密钥长度。这个需求

的原理来自这样一个事实，那就是随着时间的推移，安全专家和解译密码者会经常在网络上发现新的攻击。这一点，加上不断提高的计算能力（黑客部署的），将迫使安全管理者升级密钥的长度、修改安全策略和算法，特别是为那些保持运行很长时间的设备（如智能电表）。在某些情况下，可能会需要升级算法。在其他情况下，可能会需要发布安全补丁以解决在安装时未知的、协议和应用程序中的漏洞。同样的逻辑同样适用于可能需要不断升级的软件和固件，为了部署新特性或允许修复发现的漏洞。因此，设备生命周期管理（例如，软件和固件升级）是一个重要的 M2M 通信促成者。

4.6　M2M 中流量模型及特殊方法对网络架构设计的要求和思考

本节介绍了九种不同 M2M 细分市场（也称为 M2M 应用），它们被认为对两者都有显著的影响：

- 网络特征演变（这些演变构成了 3GPP 和 3GPP2 从事的主要工作）；
- 网络规划和尺寸方面。

尽管这张细分市场名单不是详尽的，但在我们看来它提供了一个优秀的 M2M 业务特点。本节将非常详尽地描述不同的细分市场，以及业务特征的高级特性描述。然后将为每个细分市场提供一套详细的业务水平特性，它将被用来得到一个考虑中的业务模型：

- 业务功能和相关数据的有效负载；
- M2M 模块（2G、3G 和 4G）销售预测对北美（NA）市场（作为一个相关的例子提出，在北美市场中 M2M 市场利率的水平）对于每个细分市场（来源：ABI 研究所[6]）；
- 移动网络中 M2M 模块每站点（基站）的平均集中度；
- 相对于生成的总吞吐量（考虑到网络开销和重传估计）估计的应用吞吐量。

尽管模型包含几个近似，是基于平均估计（而不是最坏的情况），但它提供了对 M2M 业务模式优秀的特征描述，允许支持正在进行的 3GPP 和 3GPP2 网络优化工作，以及运营商网络中的网络规划策略。

4.6.1　为何使用无线网络

虽然 M2M 同时适用于有线和无线，但是业务特点对无线接入网络更为重要，因为几个原因导致它的影响更大。

- 无线基础设施提供了无缝覆盖和易安装性。例如，自动售货机，越来越多地被连接到一个公共通信网络，通过铜导线或光纤连接，这个设备中有 CAPEX 和 OPEX 两种结构，这可能并不能证明通过有线设备运营效率得到了提高。然而，无

线在几乎任何地方都是立即可用的，包括室内应用。M2M 通信模块（调制解调器，允许数据和 SMS 通过蜂窝网络连接）的成本对于 2G 技术低至 25 美元（大约 20 欧元），使最初的投资相当合理。

• 虽然一些住宅和商业应用将依靠有线基础设施（主要是各种类型数字用户线路（xDSL）和光纤到户（FTTH）），但部署在住宅环境内的 M2M 设备到接入网络根本不可能是可见的（和不产生额外的重大业务量），因为这些将通常用一个网络地址转换（NAT）隐藏。与高耗带宽三合一的应用相比，额外的生成业务量通常可以忽略不计，例如视频。一些住宅部署如家庭监视将有移动电话作为主要或备份接入。除了 IP 寻址方面，几个 M2M 应用没有高的 QoS 要求，对有线网络只有非常小的负担。

作为一个结论（和超越有线对无线的比较方面），一般人都同意 M2M 在无线网络上强加了一系列的网络优化需求。因此，谈及网络优化时，本章主要集中于蜂窝网络方面。

4.7 M2M 细分市场/应用说明

基于 ETSI M2M 所做的关于用例的工作和 ABI 研究所做的研究[6]，以下部分被认为是 M2M 业务特性描述的目的。

4.7.1 汽车

汽车的 M2M 部分指的是安装在车辆里的设备项目和提供任意以下服务组合的相关网络应用。

• 汽车事故应急呼叫业务：交通事故后，向驾驶员提供自动化的援助。至今最值得注意的部署示例包括美国通用汽车 OnStar 业务，以及欧洲的 PSA、BMW 和 Volvo。对于欧洲，目前的业务提供是一个欧盟委员会 eCall 项目和相关标准（由 3GPP 开发和 ETSI 支持）的预标准实施。随着时间的推移，一般公认汽车事故应急呼叫业务将通过不同国家的规则来强制执行。

• 跟踪和交互式业务：提供车辆跟踪业务，这些业务可以由多个应用使用，包括：

- 被偷汽车的跟踪和交互停止；
- 按里程付费汽车保险；
- 租赁面积限制或基于区域分区的付款；
- 车队管理；
- 旅游信息推动；
- 基于位置的广告和商业业务。

• 交互式商业和娱乐应用：给车辆乘客提供商业（如广告）和娱乐业务。这些包括：

– 视频点播下载；
– 互动游戏；
– 交互式付款；
– 互联网接入。

很可能未来汽车的部署将由 3G 和 4G 连接控制，如果把交互和信息娱乐应用作为目标，这将尤其需要。

汽车应用的业务特征/网络影响可以被描述为

- 高移动性；
- 高数据传输率，特别是对商业和娱乐应用；
- 多承载连接。

4.7.2　智能遥测

能源部门部署智能电网和智能计量应用来达到更高程度的能源使用效率和可靠性。公用事业应用通常与部署在用户驻地的智能计量表和各种其他传感器或 M2M 设备相互作用，允许提供一个网格广泛的监控基础设施，收集消费信息和发送关于关税或奖励的信息。智能计量表和智能电网传感器将通过各种各样的有线和无线技术连接，如 PLC、网格射频、蜂窝接入等。这些提供智能计量表、传感器或 M2M 设备与公共设施后端应用、数据库和管理系统之间的网络连接。在几个欧洲国家和北美，出现了一个联合连接模型，其中从计量表到位于分布业务运营商（DSO）网络的数据集中器都使用 PLC，然后从集中器到公共设施后端应用（见图 4-4）使用蜂窝连接。可是，当每个集中器中计量表的数量超过一定的阈值（通常是 25 个），那么这种模式就仅仅在经济上是可行的。对于农村地区，一直把蜂窝带到智能计量表可以补充 PLC/蜂窝部署。

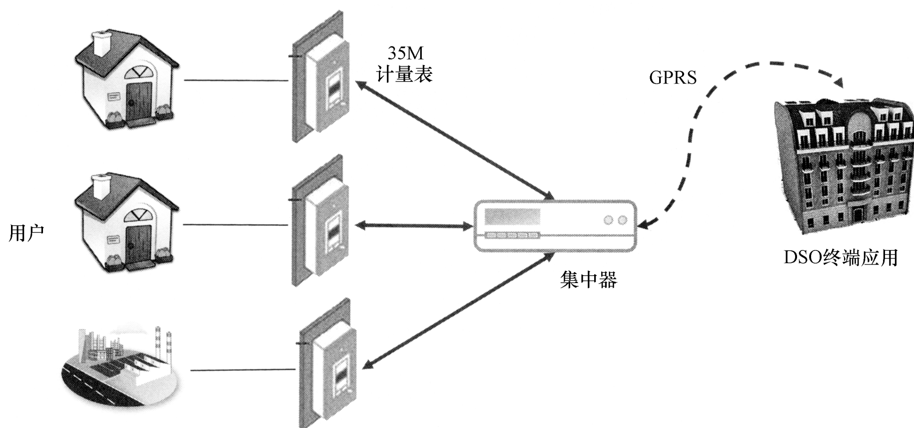


图 4-4　典型 PLC/蜂窝智能计量部署场景

智能遥测应用的业务特征/网络影响可以被描述为

- 固定设备没有移动性；
- 低数据传输率；
- 可预见的行为（一般来说，智能遥测设备被配置去定期报告数据）；
- 延迟容忍：当智能计量表被配置每个周期去报告数据（例如，每 30min），公用事业应用可以（特别是在非高峰时间）在周期内的任何时间容忍数据的报告；
- 同步效应（通常，设备被公用事业配置去同时建立连接和报告数据）。

4.7.3 监控和安全

监控和安全设备主要部署在住宅和小型商业楼宇来为安全警报应用提供图片和视频监控信息。安全设备一般使用蜂窝网络作为主要或备份接入去提供到安全监控应用或房屋所有者的连接。

交换信息大多是由报警信息和偶尔低至中等分辨率的视频信号组成。

监控和安全应用的业务特征/网络影响可以被描述为

- 没有移动性；
- 当触发警报过程时，信息周期性交换而不是不可预知的突发性信息交换；
- 偶尔业务高峰使用图片/视频传输数据时的低数据传输；
- 多承载连接。

4.7.4 销售点（PoS）

PoS 终端（包括自动取款机（ATM））提供服务，如现金分配、支付和所有收银台的任务，比如银行或信用卡支付、事务验证、销售报告和库存数据协调。

为了与大量应用交换信息，PoS 终端既与局域网相连，又与广域网相连。由于蜂窝运营商提供的广泛覆盖和易安装性，在 PoS 中使用蜂窝连接正在进行快速增长。在一些国家，所管辖的区域需要安全的和冗余的，使用有线和无线技术的连接。

PoS/数字标识应用的业务特征/网络影响可以被描述为

- 有限的移动性；
- 低数据传输率；
- 持久的承载。

4.7.5 自动售货机

自动售货机是给消费者分发商品以换取一定费用的终端。自动售货机终端正越来越多地被连接到一个网络，是为了交换有关物流和付款的信息，如通知后端应用一个特定阈值已经达到。连接自动售货机到通信网络的主要目的是通过更好的知识和需求与供应的控制提高操作效率。对自动售货机来说，由于蜂窝接入技术广泛的

覆盖，以及易于部署，所以它是占主导地位的网络连接。

自动售货机的业务特征/网络影响可以被描述为
- 无移动性；
- 低数据传输率；
- 持久的承载；
- 同步效应；
- 延迟容忍。

4.7.6　电子健康

一些电子健康应用包括以下（更多信息在电子健康用例中提供）：

- RPM：使医疗保健提供者通过远程收集、存储、检索和分析与患者相关的健康信息来监控和诊断健康状况。RPM 设备允许医疗保健提供者在病人的情况变得更加严重之前来为他们治疗，从而避免到急诊部门不必要的往返和再次到医院。最终，RPM 让住院时间大大减少，从而降低医疗保健服务的成本。通常，一个或多个传感器被用来监控病人的生命体征（如血压）。监控信息通常是使用一个常常与蜂窝网络相连的单独设备来报告。
- 个人应急响应系统（PERS）：提供给病人一个 24/7 呼叫中心接入来寻求帮助。部署的设备被挂在脖子上或戴在手腕上，并通过按一个单独的按钮来直接接入援助服务。
- MPM（移动个人监控）：非常类似于 RPM 设备，MPM 通过向中心应用报告监控信息使预防保健和健康监控成为可能。

远程治疗/医疗应用的业务特征/网络影响可以被描述为
- 低移动性；
- 低至中等的数据传输率；
- 多承载应用；
- 同步效应。

除了这些业务特征，远程健康和医疗应用经常需要网络服务提供高的可靠性和可用性；两者都可能成为服务提供者（例如，医疗保健提供者）和网络运营商之间服务水平协议的主题。

4.7.7　视频直播

视频直播通常用于应用的监督，特别是交通基础设施（公路、铁路等）或城市监控领域。视频直播摄像机被公共安全机构（例如，警察部门）或另一个与安全相关的操作中心部署来监控和记录任何与监视区域的操作有关的事件。

由于覆盖率、易部署或移动性需求，蜂窝网络构成了这个对 3G 连接（将来是

4G）有一点偏好的细分市场的技术选择，以应对视频直播的带宽需要。

视频分辨率可以考虑以下三种类型：

- 低分辨率（比特率 <128kbit/s）；
- 中分辨率（比特率 <768kbit/s）；
- 高分辨率（比特率 <10Mbit/s）。

另一个可以实现的功能是设备记录一个高清场景和根据需求转移相关文件的能力。

视频直播应用的业务特征/网络影响可以被描述为

- 固定设备没有移动性；
- 启动设备的高移动性；
- 紧急连接；
- 中到高的数据传输率。

4.7.8 楼宇自动化

楼宇自动化应用是基于用来在商业建筑中提供服务的设备。楼宇自动化系统旨在为它的居住者提供一个安全、舒适和富有成效的设施。通过降低能耗和操作人员水平，重点往往集中在运营效率。

楼宇自动化的特点是一组重要的传感器、开关、监控和遥测设备，所有的都使用网关首先连接到私有，然后连接到一个公开的有线或无线的公共网络。

应用的例子包括冷却设备的维护和监控，电梯维护和监控，电源监控等。

楼宇自动化应用的业务特征/网络影响可以被描述为

- 低或没有移动性；
- 低数据传输率。

4.7.9 M2M 工业自动化

工业自动化应用和相关设备如 PDA（个人数字助理）被用于商业和工业领域来支持一组工作流程和定义明确的业务流程。工业自动化应用可能另外收集来自遥测设备的数据。

工业自动化应用的业务特征/网络影响的可以被描述为

- 低或没有移动性；
- 低数据传输率。

4.8 M2M 交通解决方案

表 4-2 提供了 M2M 设备生成业务的不同特性。附件 A 提供了个人服务特点的一个描述。每个服务特点在业务模型中被认为是数据业务源。下一节将聚焦在智能

计量对一个典型的北美市场站点的影响上。我们将提供全球业务模型的估计，而不是详细列出所有 M2M 应用。

4.8.1　智能计量通信特性

在本节中，通过详述一个智能计量的特殊用例，我们将概述用于表征 M2M 业务的方法。我们假定了下面的典型部署结构。

在图 4-4 中，智能电表通过 PLC 连接到位于 DSO 电力网络的集中器。然后集中器通过使用蜂窝网络连接到 DSO 后端应用。对于结合的 PLC/蜂窝智能计量部署，图 4-4 反映了一种广泛采用的、被接受的模型。这个模型被假定为智能计量业务模型。

在一个智能电表或产生业务的集中器中为每个软件特性使用一个估计（按表 4-2），表 4-3 提供了每个 2G 站点每个特性平均比特率的一个估计。为了获得表 4-3中的值，主要的假设是：

- 每个站点集中器的数量为 15；
- 智能电表集中器的总数量为 100；
- 协议开销包括网络信号和 TCP/IP 为 50%；
- 单相电表的百分比为 80%（其余电表占 20%）。

表 4-3 是针对于智能计量的。为了提供每个站点的和平均基础上的整合业务模型，对每个主要细分市场已经进行了类似的研究。

依据上行和下行生成的业务，生成网络业务的每个设备特性被单独考虑。

表 4-2　M2M 设备生成业务的典型特征

汽车	智能遥测	监控与安全	销售点	自动售货机
连接/断开[①]	连接/断开	连接/断开	连接/断开	连接/断开
语音通信	每日电表读数（单相的）	日常存在控制	用户账户创建	相关销售信息交换
预警管理	每日电表读数（三相的）	预警设置	用户信息检索	预警设置
GPS 位置传送	个人读数[②]	存在检测	在线付款	读数设置
维修数据传送	负载控制和紧急情况[③]	火灾检测	预警设置	阅读事件日志，个人
固件和软件升级	预警设置	电力关闭检测	互联网接入	阅读事件日志，所有
互联网接入	读数设置	阅读事件日志，个人	阅读事件日志，个人	安全报警
电子邮件	阅读事件日志，个人[④]	阅读事件日志，所有（在某一区域）	阅读事件日志，所有	固件和软件升级
游戏/电影下载	阅读事件日志，所有	存在图片/视频下载	数据库升级	注册，认证等

（续）

汽车	智能遥测	监控与安全	销售点	自动售货机
报警管理	对家庭区域网络设备的信号控制	固件和软件升级	固件和软件升级	NTP
阅读事件日志	固件和软件升级	注册，认证等	注册，认证等	—
注册，认证等[5]	注册，认证等	NTP	NTP	—
NTP[6]	NTP	—	—	

电子健康	视频直播	楼宇自动化	工业自动化
连接/断开	连接/断开	连接/断开	连接/断开
单个参数读取	监控，QCIF 视频	每日电表读数	每日电表读数
复杂参数读取[7]	紧急视频传输 QVGA	个人读数	个人读数
视频传输（QVGA）	调查（VGA）	报警设置	报警设置
批量数据传输	报警设置	读数设置	读数设置
数据＋语言＋视频通信	读数设置	阅读事件日志，个人	阅读事件日志
设备远程认证和控制	阅读事件日志，个人	阅读事件日志，所有	固件和软件升级
报警设置	阅读事件日志，所有	固件和软件升级	注册，认证等
读数设置	固件和软件升级	注册，认证等	NTP
阅读事件日志，个人	注册，认证等	NTP	
阅读事件日志，所有	NTP		
固件和软件升级			
注册，认证等			
NTP			

① 涵盖管理设备到网络的连接和断开的所有程序。
② 与读取一大组设备的请求不同，个人接入是针对一个设备的读取。
③ 特别紧急请求控制能源需求。采取的措施可以像关闭一些设备电源一样极端。
④ 个人请求接入事件日志（例如，为了对账而进行的账单调查），而不像是对一组设备日志的接入。
⑤ 允许服务级证明、授权和注册的程序。这些程序在数据交换阶段开始之前是必要的步骤。
⑥ NTP：用于全球时间同步的网络时间协议。
⑦ 关键数据的传输需要一个高级的网络可靠性/实用性。

表 4-3　智能计量业务模型

功　能	交易量假设	活动发生每天的时刻		到终端应用（UL）					来自终端应用（UL）				
				每条消息有效负载的大小/B	数据包大小/B	每个交易的消息数量	平均比特率/(kbit/s)	忙时的平均比特率/(kbit/s)	每条消息有效负载的大小/B	数据包大小/B	每个交易的消息数量	平均比特率/(kbit/s)	忙时的平均比特率/(kbit/s)
		始	终										
每日电表读数单相	超过 30min 100%的电表	0	1	5000	1024	1	2.7	0.0	2000	1024	1	1.1	0.0
每日电表读数三相	超过 30min 100%的电表	0	1	5000	1024	2	1.3	0.0	2000	1024	2	2.2	0.0
个人读取		0	1	5000	1024	2	1.3	0.0	2000	1024	2	2.2	0.0
个人读取（忙时）		7	8	5000	1024	7	0.4	0.0	2000	1024	7	0.0	0.0
连接-断开		0	24	5000	1024	1	1.0	1.0	200	1024	1	0.0	0.0
负载控制和紧急情况		7	8	2000	1024	1	48.0	0.0	1000	512	1	1.3	0.0
报警设置		8	21	200	64	1	0.0	0.0	500	512	1	0.0	0.0
报警设置（忙时）		7	8	200	64	1	0.0	0.0	500	512	1	0.0	0.0
读数设置		8	21	1000	512	1	0.0	0.0	200	64	1	0.0	0.0
读数设置（忙时）		7	8	1000	512	1	0.0	0.0	200	64	1	0.0	0.0
阅读事件日志（个人）		7	8	1000	512	1	0.2	0.0	200	64	1	0.0	0.0
阅读事件日志（全部）		1	24	2000	1024	1	0.1	0.1	200	64	1	0.0	0.0
发送 HAN（家庭区域网络）消息		7	10	100	64	1	0.2	0.0	500	512	1	0.0	0.0
固件和软件升级		1	24	50000	1024	1	0.0	0.0	5000000	1024	1	2.0	2.0
注册，认证等		0	24	1000	512	1	0.2	0.2	1000	512	1	0.0	0.0
NTP		0	24	500	512	1	0.1	0.1	500	512	1	0.0	0.0

来源：Alcatel-Lucent。

4.8.2 全局业务特性

在本节中，我们将为2G、3G和4G业务提供全局业务特性。基于下列考虑：

- 在2G、3G和4G中全球范围的无线运营商部署特性（包括市场份额，技术部署……）；
- 依据人口密度、城市/农村知识的全球范围地理特征；
- 依据全球收入和运营商收入的全球范围经济利益率；
- 当地监管机构的推荐。

一个数据库被建立用来表示每个国家和运营商设备和应用的类别。本章余下部分中提供的业务预测假设一个有400万居民的网络应用城市，其中下表提供了M2M终端的混合（在2010年，3G和4G模块所占的百分比相对较低）：

	2012			2014		
	2G（%）	3G（%）	4G（%）	2G（%）	3G（%）	4G（%）
智能遥测	13	4	0	8	3	1
视频直播	0	1	1	0	1	1
自动售货机	1	1	0	1	1	0
电子健康	1	1	0	1	2	0
监控和安全	7	4	0	5	5	1
销售点	3	2	0	2	2	1
工业自动化	1	4	0	1	4	1
楼宇自动化	10	3	0	7	4	1
汽车	20	21	2	13	30	6
总计	56	40	4	37	51	13

4.8.2.1 2G业务

图4-5～图4-7在平均基础上提供了与2G M2M设备相互作用的M2M应用所产生的比特率（计算超过1h）。这些数据是对NA市场的一个估计，NA市场是基于对每个正在考虑中的细分市场的2G模块预计销售额。基于这些数据，可以得出以下结论：

- 2G M2M业务量在2010年到2014年之间将大约每两年翻一番。
- 全球2G模块业务量倾向于对称。虽然我们已经在前面的表中显示了，2G智能计量业务量主要表现了非对称业务量（上行和下行数据之间的平均比率是5/100），但其他2G M2M业务量更集中在下行，特别是对于汽车，其中有大量数据被下载（地图，因特网浏览，等等）。
- 在1h之内平均比特率是相当低的。峰值比率可能大得多，但很难显示，因为它取决于几个参数，如链接能力和站点负载。应用开发人员常倾向于以一个服务友好的方式构建他们的应用。例如，对于智能计量，计量表通常会被编程在开始的

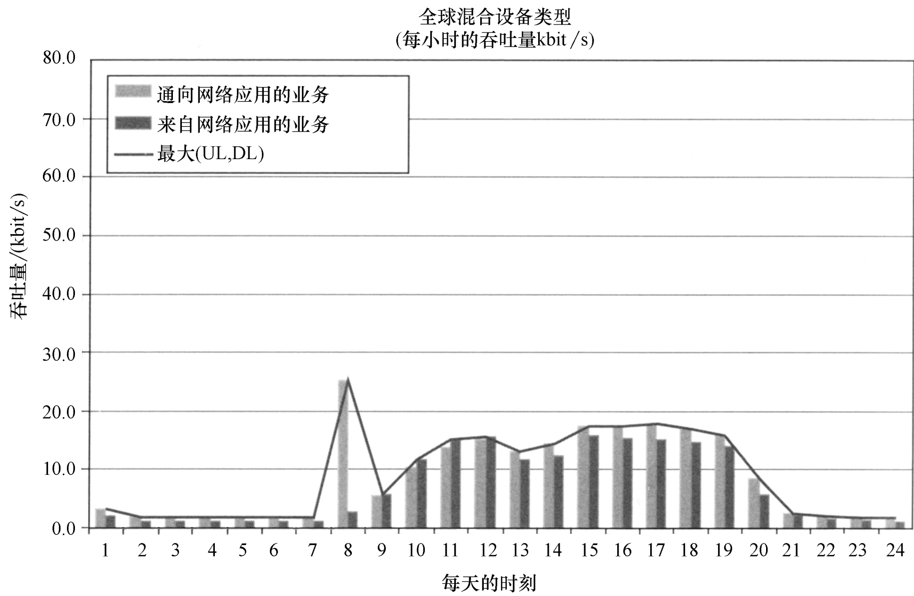


图 4-5　每个站点的平均 M2M 业务量（2G，NA，2010 年）

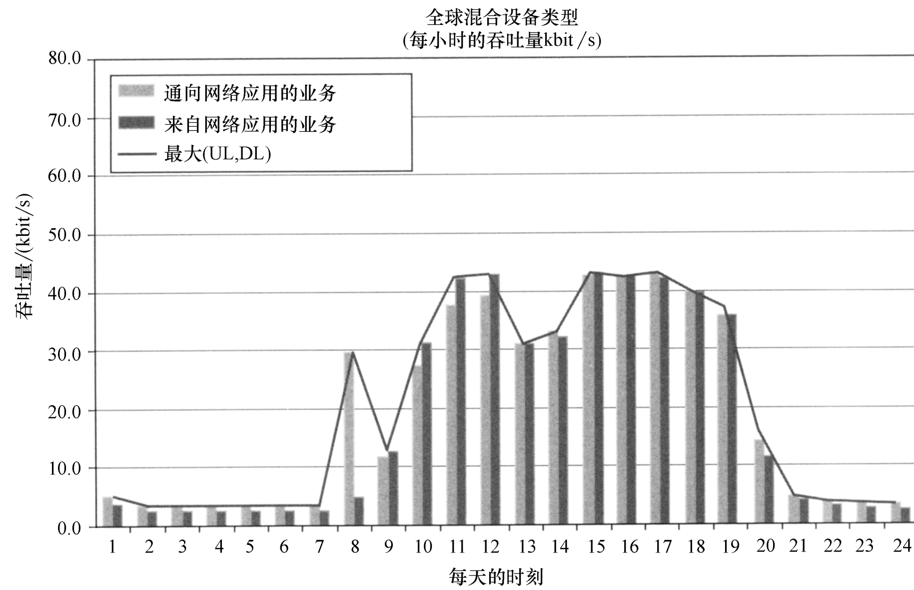


图 4-6　每个站点的平均 M2M 业务量（2G，NA，2012 年）

每小时报告数据，产生一个巨大的同步效应和网络上的一个沉重负担。这进一步如图 4-8 所述，它提供了来自运行 M2M 应用的运营网络 RADIUS 用法日常模式（协议用于身份验证和计费），这个图显示了每 90min 发生的同步效应。这个同步效应

的结果是，M2M 业务量通常产生业务量爆发，这比图 4-5 ~ 图 4-7 中显示的每小时估计比特率平均要高 20 倍。

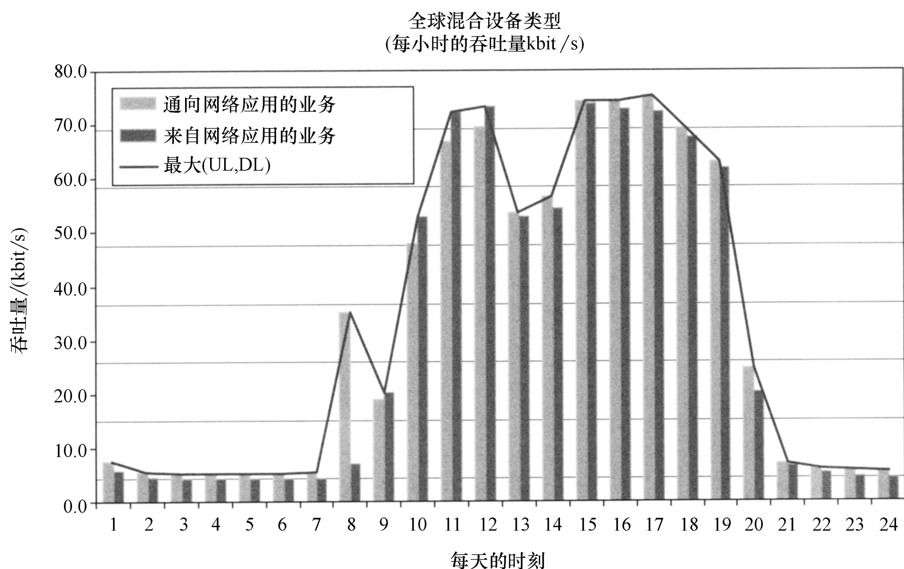


图 4-7　每个站点的平均 M2M 业务量（2G，NA，2014 年）

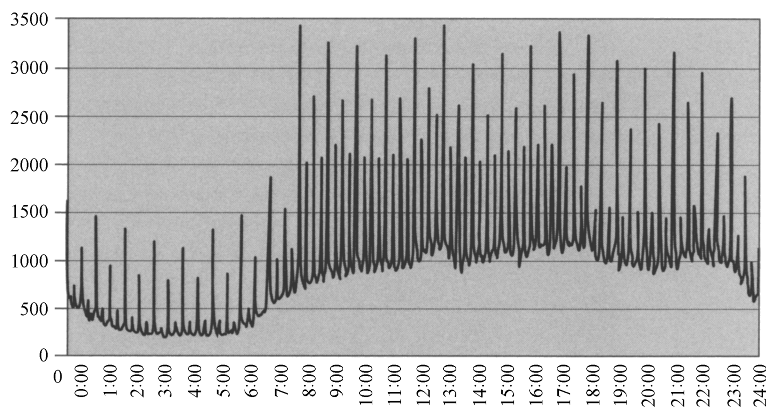


图 4-8　来自 M2M 应用的同步数据接入例子（下载到 RADIUS 服务器）

4.8.2.2　3G 业务

图 4-9 ~ 图 4-10 在平均基础上提供了与 3G M2M 设备相互作用的 M2M 应用所产生的比特率（计算超过 1h）。这些数据是对 NA 市场的一个估计，NA 市场是基于对每个正在考虑中的细分市场的 3G 模块预计销售额。基于这些数据，可以得出以下结论：

● 因为模块价格仍然相对昂贵，所以 3G M2M 业务仅仅从 2012 年才开始对网络产生重大影响。

● 相对于 2G，3G 全球业务量很不对称，其中上行业务是下行业务的 5 ~6 倍。这主要是因为一些高耗带宽应用，比如视频直播，将实际使用 3G 和 4G（当相应的模块可用时）。

● 到 2014 年，3G 全球 M2M 业务量将比 2G M2M 业务量高出 10 倍。

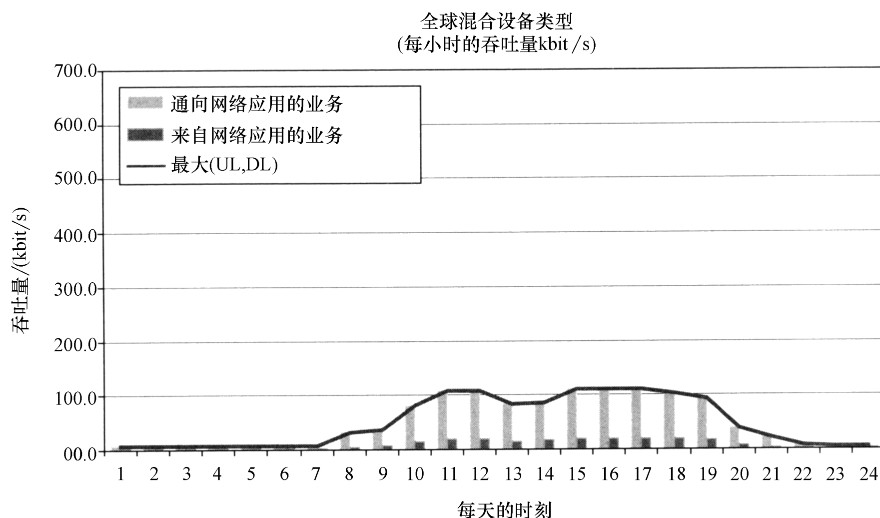


图 4-9　每个站点的平均 M2M 业务量（3G，NA，2012 年）

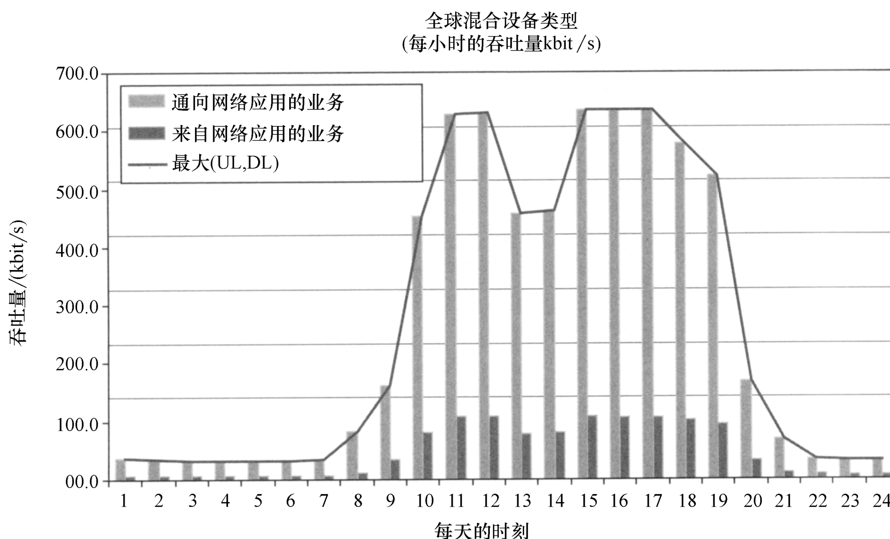


图 4-10　每个站点的平均 M2M 业务量（3G，NA，2014 年）

4.8.2.3　4G 业务

图 4-11 和图 4-12 在平均基础上提供了与 4G M2M 设备相互作用的 M2M 应用所产生的比特率（计算超过 1h）。这些数据是对 NA 市场的一个估计，NA 市场是基于对每个正在考虑中的细分市场的 4G 模块预计销售额。基于这些数据，可以得出以下结论：

- 由于 4G 模块的价格位置，相比 2G 和 4G，3G 生成业务量将占据主导地位。
- 所有从 3G 得到的其他结论对 4G 业务同样有效。
- 正如图 4-13 和图 4-14 进一步描述的一样，全球 3G 和 4G M2M 业务量是不对称的，上行业务量比下行业务量更多。这对操作部署引入了一个新的挑战，在操作部署中运营商习惯于相反的模式进行个人通信。广播和网络的设计都必须考虑到这种特性。为了下行密集型业务，目前的通信网络，以及相关标准已经被设计和优化。某些部署在 3G 和 4G 上的 M2M 应用将改变这一范式和在网络设计上强加新的挑战。
- M2M 业务是突发的，因为 M2M 应用没有按照头脑中形成的网络负载模式来开发。突发性是同步效应的结果，是由几个 M2M 设备同时报告数据造成的。
- 总的来说，M2M 混合业务的高峰时间与个人通信是相同的，即使一些 M2M 应用有一些脱节的高峰时间。因此，对于个人和 M2M 通信，网络运营商不能受益于脱节的高峰时间。因此，其他的机制，例如过载控制或延迟容忍，必须考虑以确保网络稳定和成本效率。

根据上述结论，这就表明不仅设备特性还有操作实践都必须利用 M2M 业务的所有特点，尤其在灵活性方面，以提供成本有效的 M2M 通信，控制业务负荷，避免扰乱其他需要严格服务水平协议保证的通信。

下表总结了 M2M 业务的特点，这可以被利用的条件是，“机器型通信的系统改进”，这个涵盖性术语用于 3GPP M2M 上的工作。这张表是基于提供 M2M 部分特征的前一节。

业务特征	细分市场								
	汽车	智能遥测	安全	PoS	自动售货机	电子健康	视频直播	楼宇自动化	工业自动化
无移动性	—	√	√	√	√	—	③	√	√
低移动性	—	—	—	—	—	√	—	√	√
高移动性	√	—	—	—	—	—	③	—	—
低数据率	—	√	√	√	√	②	—	√	√
高数据率	√	—	①	—	—	—	√	—	—
稳固的承载	—	—	—	√	—	—	—	—	—

（续）

业务特征	细分市场								
	汽车	智能遥测	安全	PoS	自动售货机	电子健康	视频直播	楼宇自动化	工业自动化
同步效应	—	√	—	—	√	—	—	—	—
多承载连接	√	—	—	—	—	√	—	—	—
延迟容忍	—	√	—	—	√	√	—	√	—
可预知行为	—	√	√	—	—	√	√	√	—

① 在警报的例子中，安全设备可能使用一个高数据率的承载来发送一个与警报相关的视频流。

② 有时，数据率可能是媒介，其中需要花费很长一段时间来扩大传输统计数据。

③ 对于现场直播视频设备的高移动性和其他设备的无移动性。

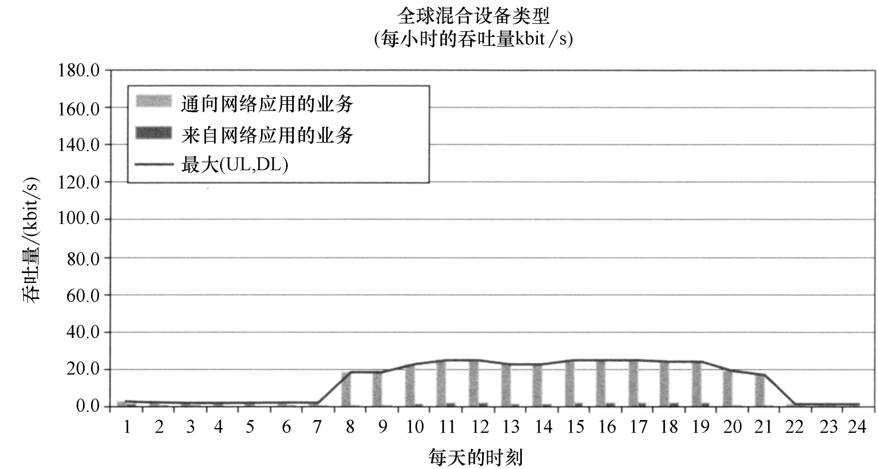


图 4-11　每个站点的平均 M2M 业务量（4G，NA，2012 年）

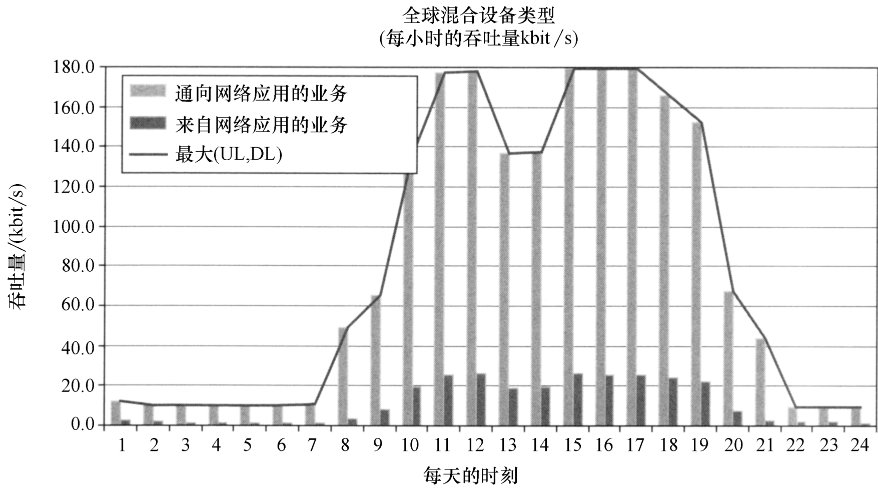


图 4-12　每个站点的平均 M2M 业务量（4G，NA，2014 年）

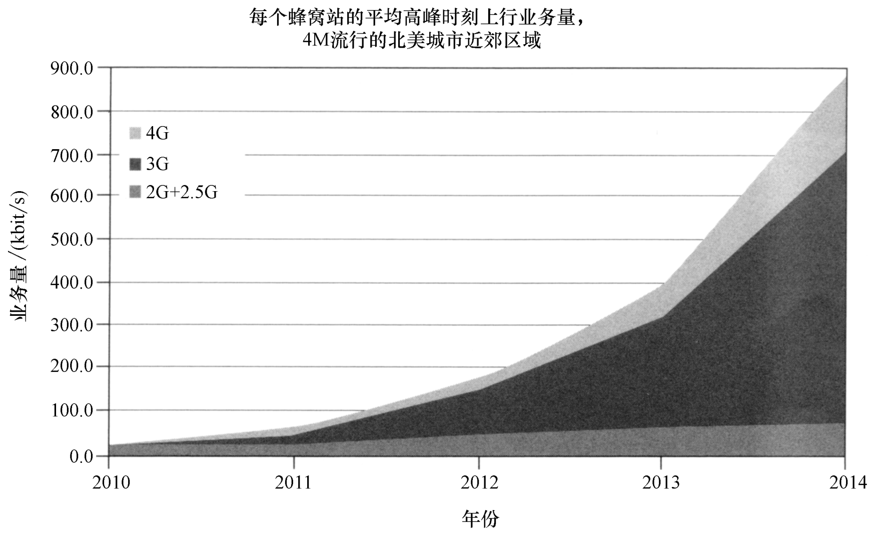


图 4-13 每个蜂窝站的平均高峰时刻业务量（上行）

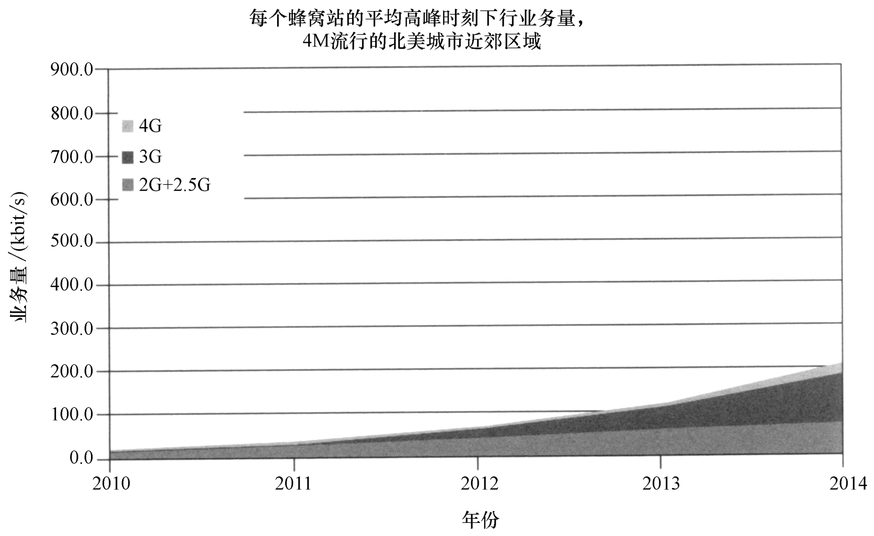


图 4-14 每个蜂窝站的平均高峰时刻业务量（下行）

4.9 M2M 通信的高层架构原则

从早期 M2M 的部署中已经吸取了几个教训。首先，垂直的整合应用很难开发、部署和测试。不仅这些需要处理应用的业务逻辑，而且它们还必须包括大量的网络感知功能。根据 M2M 应用需求，很明显，它们都依赖于一组类似的构建模

块，特别是当涉及相关通信和底层网络的所有方面。

第二，M2M 都是关于成本有效的。M2M 是以生成一小部分其他消费者手机如智能手机的 ARPU（每用户平均收入）为人们所熟知。然而，所有分析人员一致认为，部署 M2M 设备的数量将比个人通信设备高一个数量级。因此，为了提供扩展水平和匹配投影 M2M 设备和 ARPU 结构的成本，网络不得不变成 M2M 感知和利用所有 M2M 业务的特点。

图 4-15 提供了发生在不同标准化组织中工作的一个高层架构原则。它还显示了从当前部署向基于新水平平台部署的迁移计划。

图 4-15 显示了以下未来 M2M 部署的关键原则：

● 应用将越来越集中在应用业务逻辑和外包功能，比如一个设备管理的数据中介、安全、DNS、设备管理等。对这个水平平台功能的接入将通过一套开放的、标准化的和 IT 友好的 API。

● 相对于今天的垂直整合应用利用一组有限的运营商接口（主要是数据和 SMS），利用一个水平平台向一组较大的核心网络接口提供接入，如位置、QoS 和寻址，没有实施协议的负担来接入它们，因为通过使用一个单独开放的 API 隐藏了复杂性。

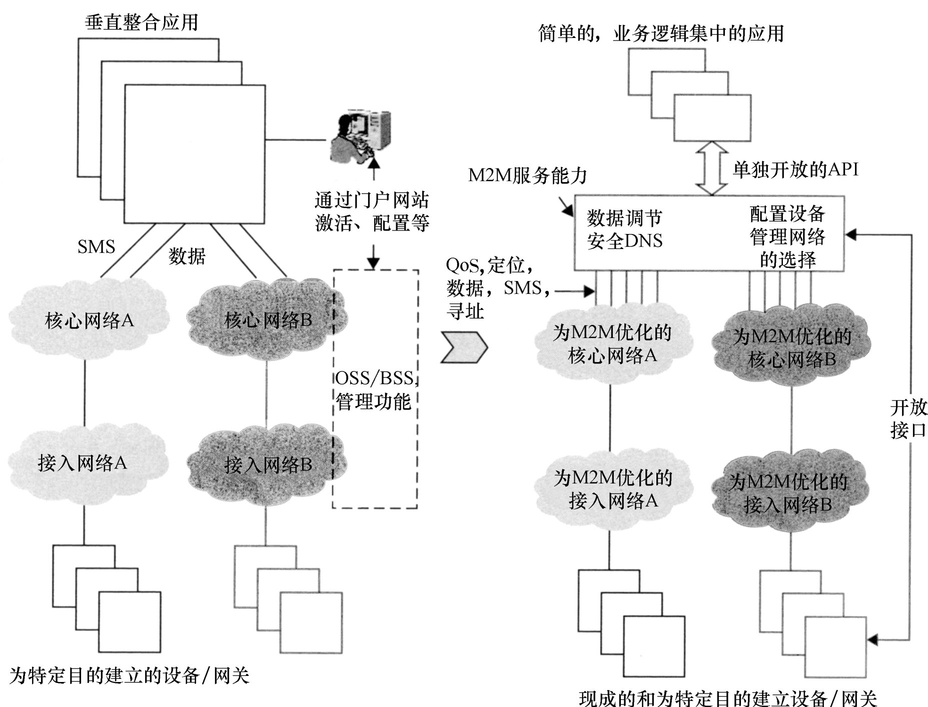


图 4-15　从最初到主流的 M2M 部署

● 接入和核心网络必须成为 M2M 感知。与水平平台上 ETSI 所做的要求需要新架构的工作相比，网络优化工作的目的不在新架构。它的目标是重新使用现有的 2G、3G 和 4G 架构（为了无线），使 M2M 业务的网络得到优化。

● 设备实现了一个对水平平台的开放界面和可能配备现成的功能来实现网络水平平台同样的功能：M2M 业务功能。设备客户端应用将得到这些业务功能，网络方面也会得到。

为了提供一个网络优化方面高水平的概述，以下提供了被 3GPP 标准化的功能的例子[3]：

● 低移动性：用于 MTC（机器类通信）设备，它不移动、很少移动或者只在一个特定的区域内移动。优化包含较少频率的（基于运营商政策）引发网络资源消耗的移动性管理功能。

● 时间控制：用于 MTC 应用，可以容忍只在定义的时间间隔发送或接收数据。网络运营商可能会允许这样的 MTC 应用在这些定义的时间间隔之外发送/接收数据和信号，但对这样的业务，计费是不同的。

● 时间容忍：适用于 MTC 设备，可以在网络过载阶段推迟它们的数据传送以换取更好的速率。

● 仅分组交换：适用于 MTC 设备，它只需要分组交换的服务，这意味着不需要接入 SMS 或电路语音服务。

● 较少的在线数据传输：适用于 MTC 设备发送或接收少量的数据。目的是当有限数量的数据被发送时极大地减少了信号过载。

● 优先警报消息（PAM）：用于在发生如盗窃、破坏公物或其他需要立即注意的情况时，MTC 设备发出一个优先级的警报。

4.10 本章小结

本章提供了一个有关网络发展的 M2M 要求，以及业务架构的概述。它清楚地表明 M2M 在网络上强加了非常具体的需求以实现更低的投资和匹配 M2M 通信强加 ARPU 限制条件的运营成本。根据广泛的 M2M 用例分析，本章做了一个案例，明确地需要部署一个水平架构作为一种减少新的 M2M 应用开发、部署和测试成本与时间的方法。这样一个水平平台还提供更容易地向网络使能者的接入，例如位置、QoS 和寻址，否则这很难接入，因为接口的多样性和与多个运营商建立商业关系的复杂性。

接下来的章节将更加深层次的关注 3GPP 中正在进行的网络优化工作，以及 ETSI M2M 平台架构工作。

参考文献

1. TR 102 691. ETSI Technical Report, Machine-to-Machine Communications (M2M); Smart Metering use cases (05-2010).
2. Smart Meters Coordination Group Standardisation Mandate to CEN, CENELEC and ETSI in the Field of Measuring Instruments for the Development of an Open Architecture for Utility Meters Involving Communication Protocols Enabling Interoperability M/441, final report (Version 0.7, 10-12-2009).
3. TR 23.888. 3GPP System Improvements for Machine-Type Communications (Release 11 – to be published 2012).
4. TR 102 732. ETSI Technical Report, Machine-to-Machine Communications (M2M); eHealth use cases (to be published 2012).
5. ETSI TC M2M Service Requirements for Release 1, published 08-2010.
6. ABI Research Study (2009) Cellular M2M Markets.

第 5 章　ETSI M2M 业务架构

Omar Elloumi[1]，Claudio Forlivesi[2]
[1]Alcatel-Lucent，Velizy，France
[2]Alcatel-Lucent，Antwerp，Belgium

5.1　引言

M2M 承诺在每一个视域的物质化层面花费更多的时间。早期阶段，一直致力于对视域进行重新定义，测试新的商业模式，开发独立的解决方案，以测试概念的可行性，并且克服了不足的互操作性的局限性。水平业务平台的应用是 M2M 视域的一个组成部分，它对于操作者来说作为一种提供增值服务的方式，或者作为一个应用提供者来生成一种模块化并且面向未来的应用性支持策略。最近来自扬基集团在美国的运营商关于 M2M 的报告指出，一种密切关注 M2M 的运营策略，非常清楚地体现了一个事实，那就是在垂直平台的基础上提供增值服务对通信运营商来说已经成为企业的当务之急：

在运营商看来，增值服务就好比新的差异性。美国的四个主要的运营商已经扩大了他们的覆盖范围，网络的可用性作为一个关键的差异性正在降低。重叠覆盖区域提高了价格竞争，由于解决方案供应商在许多地区有很多运营商选项，并且会在每个合同的基础上因为最低价格而货比三家。为了吸引客户，四大运营商之间的趋势是将促进灵活、简单的渠道和强大的设备管理服务。

（来源：扬基集团）

这样一个水平平台的组件也许会在有针对性的 M2M 应用的基础上变得多样化。例如，支持位置服务对车辆跟踪应用而言是必须的，但是对智能电表却未必需要。另外，一种阶梯式方法正在被那些致力于部署水平 M2M 平台过程的运营商所采用。原来的重点是将连接和激活、基本的数据调解、设备管理和安全作为主要目标。图 5-1 对 M2M 基本的水平服务平台组件做了一个概括。这些组件主要包括以下几类。

- 数据调解功能：允许基本的数据采集、存储，以及有关数据可用性的事件订阅/通知。另外，更深层次的复杂数据功能将会被提出，例如数据聚合和数据分析。
- 通信：隐藏网络将应用向特异性以及通信协议过渡。通信功能包括名称到网络地址转换，载体选择（SMS，数据载体）和编制，协议转换，等等。

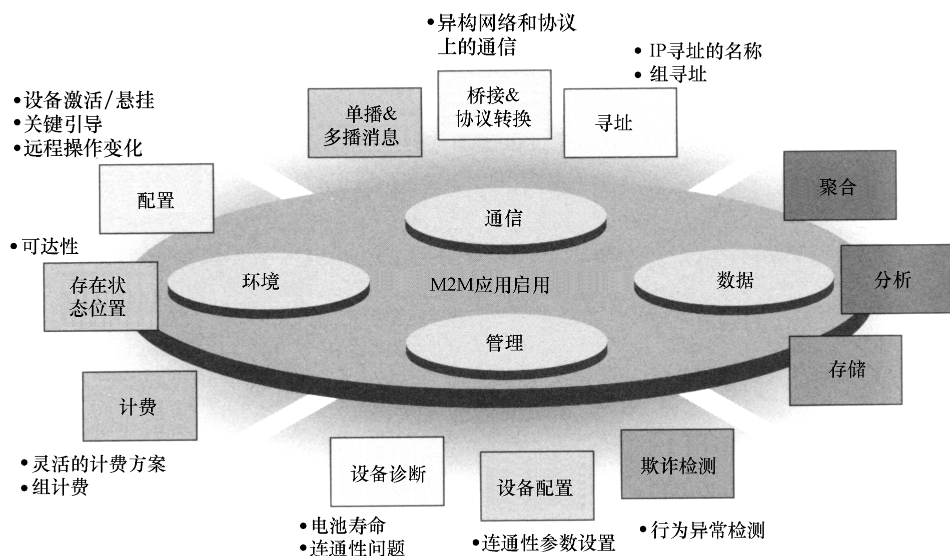


图 5-1　一个水平 M2M 服务平台的典型组成部分
来源：扬基集团

● 管理功能：提供具有配置管理（CM），故障和绩效管理（PM）（例如电池电量监测）以及固件和应用软件升级的应用。管理功能是 M2M 的一个重要组成部分，尤其是要考虑 M2M 设备的相对较长寿命的时候（对智能电表而言多于 20 年）。

● 环境：提供到其他功能例如位置、配置（设备激活，安全性关键的引导，等等）和计费功能的入口。

本章将重点介绍在 ETSI 技术委员会机器对机器（ETSI TC M2M）中标准化工作的产生。技术委员会的目的是为这种水平平台的部署提供一个基于标准化的基础。

本章的结构如下。首先，提供了高层次的系统架构，并介绍了用于构建水平平台服务能力（SC）的通用框架。这个框架进行进一步的检查，以显示个性化的服务功能。因为这个主要功能还给出了一种激励和功能说明。其次，对有关表述性状态转移（REST）和加强 REST 作为一种架构模式应用的动机做了介绍。本章其余部分主要集中在资源结构，以及接口程序，用一个例子来解释。

5.2 高层系统架构

高层系统架构对系统的组件，以及单个组件之间的附属给出了一个概括。为了描述功能体系结构，它提出了一种阶梯式方法的初始观点。架构的第二个层面是对系统内各功能之间的相互作用提出了一个更正式的描述，其中每个功能都可以被映射为高级系统架构的组件。

ETSI TC M2M 已采取以下的高层系统架构，它允许系统根据标准化有共同的理解（见图 5-2）。这个高层次的体系结构完全支持对 M2M 服务能力的需要，这种服务能力充分体现在应用程序、网络、设备或者网关。提供一个 M2M 系统的端到端表示是这个高层系统视图的一个重要组成部分。然而，不是这个体系的所有元素在 ETSI TC M2M 中由于标准化工作都具有针对性。该结构充分认识到 M2M 通信将最大程度地利用已经部署的接入和核心网络，以及任何其他形式的本地和个人区域网络。另外，在 3GPP 和 3GPP2 中关于 M2M 目前正在进行的移动网络的改进被认为是提高 M2M 服务的交付手段，而不是必须具备的功能。这样，ETSI TC M2M，至少在版本 1 中有它的一套规范，对 M2M 而言不再依靠目前的 3GPP 和 3GPP2 网络的改进，因为实现必须基于现有的网络部署。然而，我们也希望随后的 M2M 标准的发布将会加快寻求优化这些网络改进。

M2M 高层系统架构（见图 5-2）包括 M2M 设备领域的概念，以及网络和应用领域。

M2M 设备领域包括以下元素：

● M2M 设备：一个运行 M2M 应用的设备，在本章的其余部分被简称为设备应用（DA），运用 M2M 服务能力和网络领域的功能。M2M 设备可以以下面的方式连接到 M2M 的核心：

– 方案 1 “直接连接”：M2M 设备配备有一个 WAN 通信模块，并直接接入运营商接入网络。这种装置的例子包括一个直接连接到 GSM/GPRS 基础设施的智能电表。在这种情况下，M2M 设备执行程序，如注册、认证、授权、管理、网络配置和应用领域。

– 方案 2 “网关作为网络代理”：M2M 设备通过一个 M2M 网关连接到网络和应用领域。M2M 设备通过运用 M2M 区域网络连接到 M2M 网关。这种情况适用于“低成本” 设备，这种设备仅仅运行应用，并且在 M2M 网关中充分利用 M2M SC，以便执行如在方案 1 中相同的程序。

● M2M 区域网络：一个通用的术语，指的是任何网络技术。在不同的 M2M 设备之间提供物理层和 MAC 层连接到相同的 M2M 区域网络，或者允许 M2M 设备通过一台路由器（图 5-2 中没有显示）或一个网关接入到公共网络。M2M 区域网络

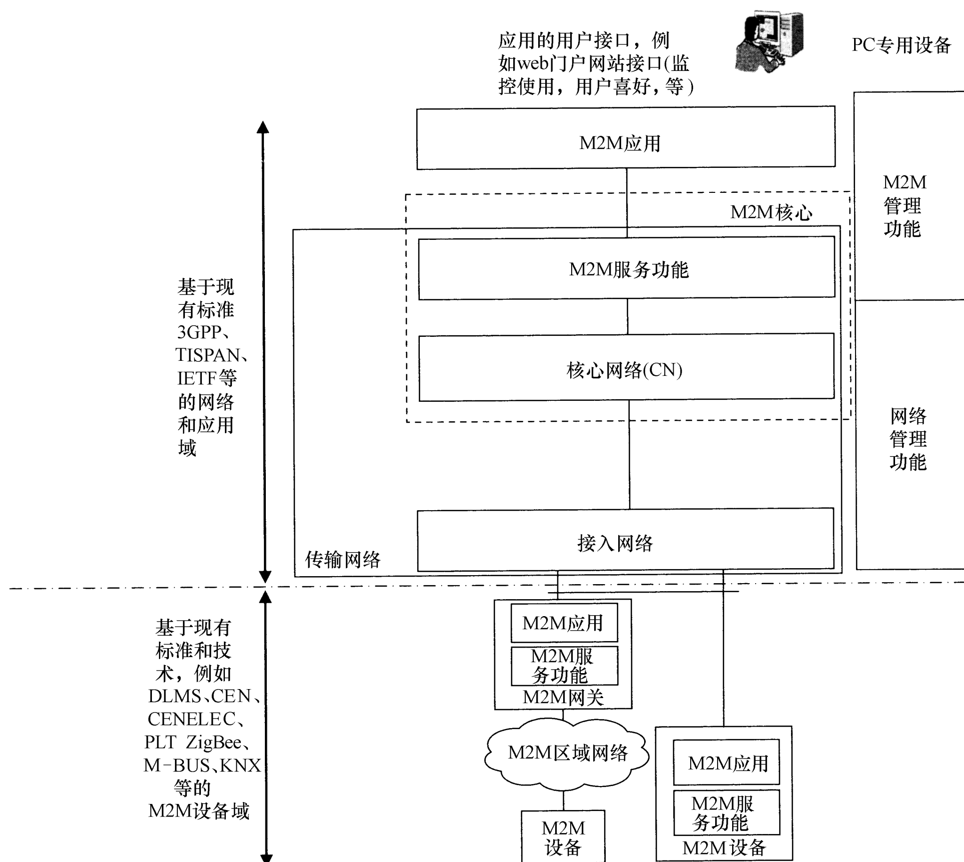


图 5-2 M2M 高层系统架构概述。由 ETSI 许可转载

的例子包括无线个人局域网，例如 IEEE 802.15.x、ZigBee、蓝牙等，或者本地网络，例如 PLC（电力线通信）或者 WiFi。然而一些 M2M 区域网络是基于无线 RF（射频）技术的，其他的有线技术也正在被考虑。PLC 之外，最显著的例子是 G.hn 家庭标准［G.hn］，此标准设计的目标是提供了多个配置文件，适用于多媒体/高带宽应用和基于低带宽要求的低复杂度终端。后一种选择自然地适用于 M2M 应用，如归属能源管理。

● M2M 网关：网关设备实现 M2M SC 以确保 M2M 设备对网络和应用域之间的相互作用和相互附属。M2M 网关可能会运行 M2M 应用。这是一个典型的设备，除了一个或多个允许接入到 M2M 区域网络（例如，ZigBee、PLC 等）的通信模块之外，至少有一个 WAN 通信模块（例如，GSM/GPRS）。M2M 网关可以实现本地智能，例如，激活来自各种消息资源（如来自传感器和环境参数）的收集和处理的自动化过程。

网络和应用域由以下元素组成。

- 接入网络是一个允许 M2M 设备域与核心网络进行通信的网络。接入网络的例子包括 xDSL、HFC、卫星、GERAN、UTRAN、eUTRAN、W-LAN 和 WiMAX。
- 传输网络是允许数据在网络内部和应用域之间进行传输的网络。
- M2M 核心重新组合各种 M2M SC，这充分体现了网络应用（NA）以及运营商的核心网络。

  – 核心网络提供有关连接性和服务的功能，以及网络控制功能（例如 3GPP PCRF㊀、SMC-SC 等）和与其他网络的互连功能。

  – M2M 服务能力（SC）提供 M2M 功能，这些功能通过一组开放的接口来体现 NA。M2M SC 通常通过已知的和标准化的接口使用核心网络功能，这些接口例如 3GPP Gi（用于 IP 数据通信的交换）或 3GPP Rx（用于接入 QoS 控制功能）。M2M SC 通过嵌于 M2M 设备或 M2M 网关上同等的 M2M SC 相互影响服务水平。

- M2M 应用程序运行业务逻辑，并且凭借一个可接入的开放的接口使用 M2M SC。M2M 应用在网络和应用领域的例子包括有多种用途的负责收集和分析智能电表数据的后端应用。
- 网络管理功能是所需的管理接入、传输和核心网络的所有功能。这些包括（但不限于）配置、监督和故障管理（FM）。
- M2M 管理功能是要求管理在网络与应用域中的 M2M 应用和 M2M SC 的所有功能。M2M 设备和网关的管理可以使用 M2M SC。

在网络和应用领域以及设备域中，M2M SC 是 ETSI TC M2M 工作的基石。标准化工作的主要目标是：

- 识别充分体现在应用的功能，以及 NA、网关应用或 DA 的功能。
- 规范垂直界面（也称为 API），允许应用充分利用 M2M SC。
- M2M SC 之间在服务级别的标准化水平接口。
- 确定 SC 如何在网络和应用领域充分利用核心网络的功能（但此项目在 ETSI TC M2M 规格的版本 1 中尚未完全解决）。

为了允许 M2M SC 的一个可扩展的和灵活的结构，ETSI TC M2M 已经选择开发一个 SC 框架。在下一节中给出了这一框架的概述。

㊀ 策略和计费规则功能（PCRF）是一个服务器，提供对网络用户的策略决定。这些策略一般与 QoS 级别和计费规则有关。

5.3　ETSI TC M2M 服务功能框架

一个框架就是一个有结构的工具箱，其根据架构或一组可以被实例化的设计模式来实现特定的目的。在 ETSI TC M2M 环境中，该框架是 SC 的骨架，并且是系统的不同实体之间的一组参考点。该骨架通过一组特定的 SC 实例化，从而使基准点构成初始的占位符用于 M2M 系统实体之间的交互协议。这个框架充分考虑了可扩展性，因为不是所有的 SC 在标准规范时都熟知，也不是对一个执行部署的所有功能强制性。为了在 SC 中通过应用避免拥塞，对于面向未来的标准化和操作的灵活性，这种能力是很重要的。

图 5-3 指出该框架被用于构建 ETSI TC M2M 架构。无论是在网络和应用域还是在设备域，它展示了一个业务层架构，这个架构由一系列 SC 表达。该框架展示了一系列基准点，整理如下：

- 在设备/网关或者在网络中，垂直参考点代替应用。
- 在设备或网关中的 SC 和在网络服务水平上的 SC 之间存在一个单独的水平参考点，这意味着它在 M2M 区域网络以及接口和核心网络使用可用的网络连接。
- 一组垂直接口连接核心网络，这是为了满足充分利用运营商核心网络功能的要求，这些接口包括关于数据的 3GPP Gi/SGi 或通过核心网络提供 3GPP Rx 到 QoS 的接入［3GPP TS 23.060，3GPP TS 23.401］。

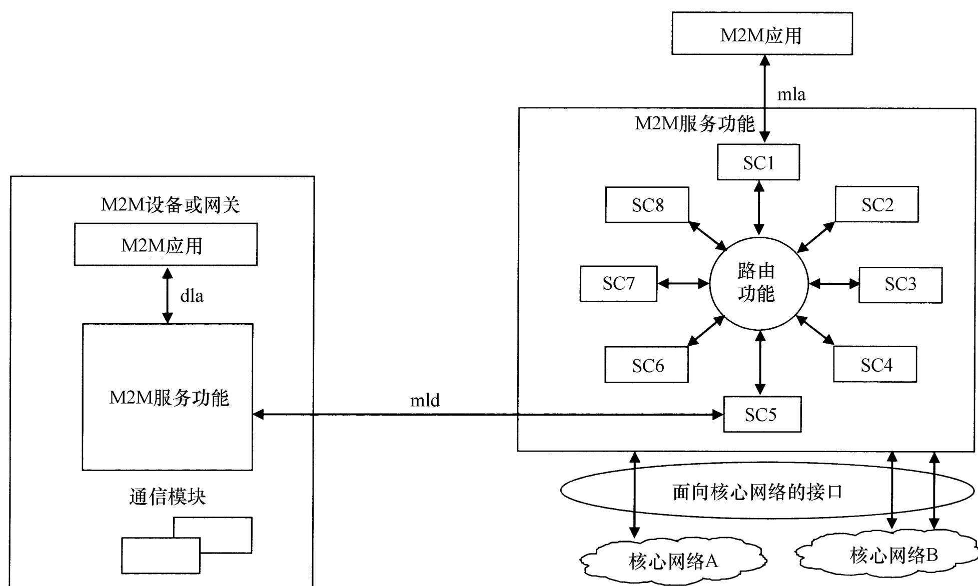


图 5-3　M2M 服务功能的功能架构框架。由 ETSI 许可转载

服务功能提供由不同的应用共享的函数；这些都是提供特定服务的软件模块，比如特定设备的位置。注意在ETSI中架构的定义是功能架构，而不是箱（box）架构，这意味着一个或多个SC可以分组。ETSI TC M2M架构不强制要求一个特定的SC实现，只要根据参考点规范SC的外部行为。

网络和应用域中的SC可以与多个核心网络连接。

ETSI TC M2M标识M2M版本1规范集的以下功能（尽管在规范集的版本1中没有通过标准化将所有的SC充分体现）：

- 应用支持（xAE）提供了一个连接应用程序的单独API接口。
- 通用通信（xGC）管理所有方面，包括相关安全传输会话的建立和拆除，以及由核心网络提供的与承载服务的连接。
- 可达性、寻址能力、知识库性能（xRAR）为状态相关的应用、设备和网关提供存储能力以及处理数据变化订阅。
- 通信选择（xCS）为通过多个网络或者是多个连接承载而完成的设备或网关提供了网络和网络的承载选择，例如，WiFi或GPRS。
- 远程实体管理（xREM）提供有关的设备/网关生命周期的管理，如软件和固件的升级，故障和性能管理。
- 安全（xSEC）实现引导、身份认证、授权和密钥管理。例如，与一个M2M认证服务器（MAS）连接（例如通过放大率）来获得认证数据。
- 历史和数据保留（xHDR）（任选）存储记录有关的M2M SC用法。xHDR可以用于执法目的，比如隐私。
- 事务管理（xTM）（任选）管理事务。
- 补偿代理（xCB）（任选）管理代表应用的补偿交易。
- 通信运营商接触（xTOE）（任选）提供接入，通过相同的API用于接入SC，传统的网络运营商服务，例如SMS、MMS、USSD和位置。
- 互通代理（xIP）根据ETSI标准允许非ETSI兼容的设备互通。

上述中的未知量分别代表如下：

- N表示网络。
- G表示网关。
- D表示设备。

ETSI TS 102690采用以下术语在网络、设备和网关中提到SC。

- NSCL：网络服务功能层在网络和应用域中涉及M2M SC。
- GSCL：网关服务功能层在M2M网关中涉及M2M SC。
- DSCL：设备服务功能层在M2M设备中涉及M2M SC。
- SCL：服务功能层是指以下几个方面：NSCL、GSCL、DSCL。
- mIa参考点：允许应用接入网络和应用域中的M2M SC。

● dIa 参考点：

– 允许嵌入 M2M 设备的应用接入在相同的 M2M 设备或一个 M2M 网关中的不同 M2M SC。

– 允许嵌入 M2M 网关的应用接入相同 M2M 网关中不同的 M2M SC。

● mId 参考点：允许 M2M 设备或 M2M 网关与在网络和应用域中的 M2M SC 进行通信，反之亦然。mId 将核心网络连接功能作为一种基础传输来运用。

5.4　ETSI TC M2M 的版本 1 方案

本节对那些目前在 ETSI TC M2M 中有考虑的方案，提供了一个更深入的讨论，并且解释了它们对指定参考点的使用。这些方案如图 5-4 所示。

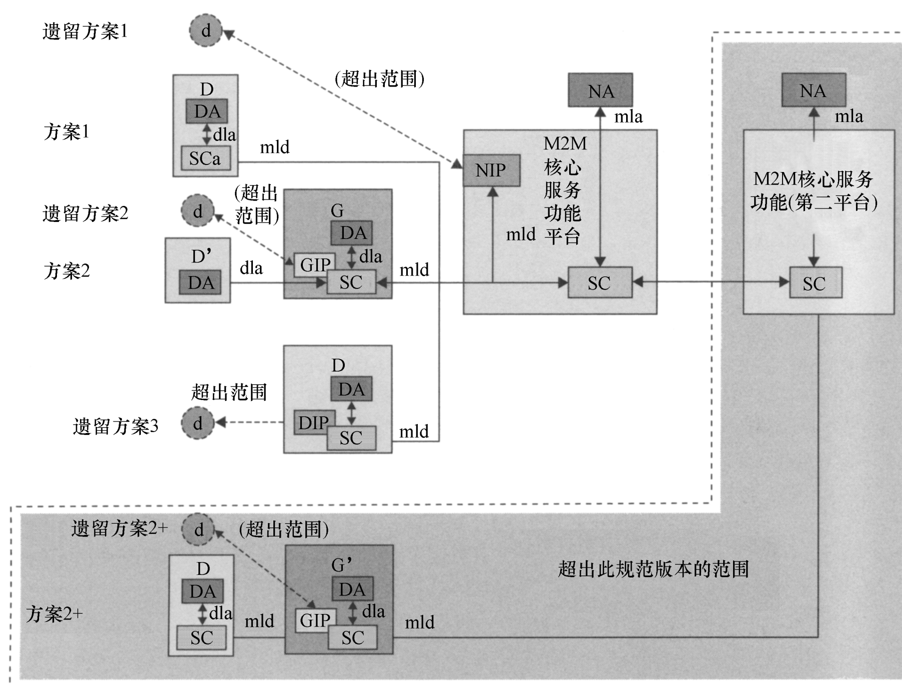


图 5-4　服务功能的功能架构框架。由 ETSI 许可转载

下列设备类型在图 5-4 中有考虑：

● 网关（G）是一个 ETSI M2M 设备，专门用来直接管理 ETSI M2M 设备的 M2M 区域网络；网关通过 mId 参考点与 ETSI M2M 核心网络直接进行通信。

● 设备（D）是一个 ETSI M2M 设备，它能够与 ETSI M2M 核心网络或 ETSI M2M 网关直接通信。

• 设备′（D′）是一个 ETSI M2M 设备，其不能实现 ETSI M2M SC。它通过 M2M 网关（G）中 SC 的应用与 M2M 核心直接相连。

• 网关′（G′）是一个 ETSI M2M 网关，它与 D 和 D′设备相连。注意，G′在 ETSI TC M2M 版本 1 规格中未被处理。

另外，由 ETSI M2M 兼容设备或网关实体管理的 M2M 区域网络有一个非 ETSI M2M 兼容设备（d）。（d）类型设备不能直接接入 M2M SC。然而，通过 xIP（互相配合代理）ETSI 兼容实体的互相配合是可能的。

在图 5-4 中描述了以下方案：

• 遗留方案（遗留方案 1、2、3 和 2 +）涉及传统的移动设备，简称为“d”的移动设备（低级方案 d），这不是 ETSI TC M2M 兼容。可以通过 xIP 服务能力将这些设备集成在 ETSI TC M2M 架构中，此处的 x 可以是 N（网络）、G（网关）或者 D（设备）。xIP（NIP，GIP，DIP）是一种特殊能力，它可以通过 mId 参考点的实现使一个非兼容设备看起来像一个 ETSI 兼容 M2M 设备。注意，然而 ETSI TC M2M 规范没有规定如何进行互通。这种互通的细节没有得到规范，并且具体实现也没有记录。

• 方案 1 体现了一个 D 设备，它被定义为一种实现 M2M SC 和运行 DA 的装置。D 设备在网络和应用域与 M2M SC 连接，充分利用 mId 参考点。

• 方案 2 展示了一个 D′设备，它是一个 ETSI TC M2M 兼容设备，但不完全实现 M2M SC。也就是说，通过 dIa 外部（此方案中）参考点，在 M2M 网关中它依附于 SC，网关简称为“G”。

• 方案 2 + 涉及通过网关 G 在网络和应用域中 D 设备与 M2M SC 的连接。这种情况下的动机是允许一个 D 设备使用 WAN 连接，但在需要的时候——例如，移动设备方案中——重复使用网关提供的现有 WAN 连接。

5.5 ETSI M2M 的服务功能

本节提供了最重要的 M2M SC 的选择和描述。目的并不是提供一个详细的描述，而是专注于最重要的特性，以及其介绍背后的哲理。本节还介绍了如何将这些功能分别在不同的网络、网关或设备实现。

5.5.1 可达性、寻址能力、知识库性能（xRAR）

xRAR 是 ETSI TC M2M SC 工作的基础。这将导致在 ETSI TC M2M 工作的早期阶段介绍的两种其他功能合并：

• 设备应用程序库：最初引入是为了保持一个注册 DA 的记录。

• 命名寻址和可达性：最初引入是为了提供地址转换功能，并且为了跟踪设备

的可达性状态或者这些设备上的应用运行。

这两种功能的合并，导致 xRAR，简化了结构，并且避免了两个功能之间不必要的频繁的消息交换的需要。

新定义的 xRAR 特性围绕 SC、应用（NA，DA，GA），以及最重要地按照接入权利和权限 M2M 应用系统之间的数据交换简易化的注册信息的维护。

需要存储的数据，并提供给其他应用最终成为 xRAR 的最重要特性。这种需要的动机如下：

如果一个 M2M 设备（并因此驻留的应用）并不是一直运行，它会变成不可达的。但是，在有些情况下，应迅速返回其最后的采样。如果 DA 及时使可利用的数据采样作为一个动态文件存储在一个 web 服务器，那么 DA 的最新状态始终可以接入。xRAR 是 SC，其允许数据的调解，而不一定需要保持唤醒周期来管理复杂的机制。

在这个机制的基础上，为网络应用提供订阅成为可能，并且当相关数据（匹配特定订阅标准）生成时被触发。

以下是 xRAR 的功能列表：

- 提供名称（设备、网关或应用）与网络地址之间的映射，例如，IP 地址，以允许对应的实体名称的连通性。
- 维护 M2M 设备或 M2M 网关的可达性状态，以及未来计划的唤醒时间和持续时间（适当应用的 NRAR——网络域中的 xRAR 实例化）。当设备或网关为了接受传入的连接得到配置，此功能是有用的。
- 提供了一种机制，其允许应用或 M2M SC 注册，并且通知一个特定的事件发生，例如，数据变得可用。
- 允许创建一组 M2M 设备、应用或 SC，让 xRAR 的用户之间进行简单的互动。例如，NA 将一个信息发送到一个组比发送到组的单个成员更容易。
- 允许应用存储应用数据，并且与其他应用一致共享接入权限和授权。
- 允许本地应用注册，通过 M2M SC 为初始化数据交换设定的前提。本地应用的一个先决条件是指用于网络服务功能（NSC）的 NA、设备服务功能（DSC）的 DA 或在 D′设备中运行的 DA 的网关服务功能（GSC），并且最终 GA 代替 GSC。
- 允许 SC 共同注册，作为应用先决条件上的数据交换前提。

5.5.2　远程实体管理性能（xREM）

xREM 在 ETSI M2M 中会被介绍，为了提供管理设备和网关生命周期的方法。M2M 设备和网关安装了很长一段时间，这简直是不可能的假设，它们运行的软件是稳定的，而且包括所有满足可预见未来的功能需要。此外，M2M 设备或网关可能会运行多个应用，而其中一些应用在设备部署之后被很好地安装。美国的智能电

网解决方案，例如，意识到升级部署的智能电表软件的必要性，并分配一个专用的PAP（优先行动计划），目的是在驱动相应的配套标准。以下是本文提到的PAP范围：

先进计量架构（AMI）和智能电表的投资如今作为先导，或实现额外的智能电网、能源管理和消费者参与活动。

这些电力公司和监管机构面临的关键问题之一是需要确保由应用选择的技术或解决方案将是可互操作的，并且符合尚未建立的国家标准。

（来源：http：//collaborate. nist. gov/twiki- sggrid/bin /view/Smart grid/PAP00 MeterUpgradability）

设备生命周期管理包括以下几个方面：

• 软件和固件升级，其中，在此环境中，该软件是普遍适用的操作系统，软件模块执行 M2M SC 和相关的 API，而该固件是软件的特定部分，往往紧凑，控制该装置的各种电子部件。

• 应用生命周期管理-能够安装/删除应用或升级现有的应用的新版本。

• 故障和性能管理，适用于检测故障有关设备的所有组件（软件或硬件），以及监控性能指标。故障和性能管理的最终目标是采取纠正措施，以确保在可能情况下，服务的连续性。例如，如果一个 M2M 设备是由电池供电的，它对检测电池的状态是有用的，并确保该进程，允许及时的电池切换触发，以便阻止服务中断。其他参数包括 CPU 或内存使用量可以被监测。

• 配置管理（CM）适用于设置设备的不同参数，为了允许其适当的操作。在 ETSI TC M2M 的环境中，CM 适用于与设备组件相关的任何参数，诸如 USB 接口或照相机等。

5.5.2.1 设备管理动机

• 设备管理包括复杂的操作，主要是正交到应用的业务逻辑。例如，在此情况下，一个软件的新版本是不正确地运行。在这种情况下，设备管理程序可能需要对软件的旧版本执行回滚。回滚是一个复杂的过程，为了在设备和网络中得到保持，其需要特殊的专业知识和可能的复杂的状态机。

• 设备管理可以受益于更好地了解网络特性。大量设备的软件升级在很长时间可以预定。因此，如果安排在非繁忙时间，升级可能受益于网络诱因。另外，如果由网络运营商提供，它可以考虑到实际的网络负载，从而不破坏更多的 QoS 敏感业务。

• 应用不需要知道所使用的设备管理协议的细节。在大多数当前的部署，设备管理使用成熟的技术，如 BBF TR069（BBF TR069）或 OMA 设备管理（OMA DM）。两个协议都有自己的特殊性。例如，最新的 OMA DM 部署要求设备通过发送一个特殊的 SMS 到设备，建立设备管理会话。另一方面，在 BBF TR069 情况下，在没有 SMS

等效的有线环境中主要地应用，需要其他机制来触发装置建立管理会话。

● 简化的故障和性能管理假设设备管理功能包括监测电池的状态。输送所有的电池参数（特别是消耗水平）将不利于 NA。通常情况下，NA 只会对达到一定阈值时的通知感兴趣，为的是安排和计划维护周期。同时，NA 可能会对电池是否被太快耗尽的通知感兴趣，以便尽可能地解决这个问题。

NREM 的 ETSI TC M2M 规范列出了以下为 NA 提供的功能：

● 提供了配置管理（CM）功能，比如一个设备外围的配置。

● 采集和存储性能管理（PM）以及故障管理（FM）数据。当预配置的事件发生时通知 NA，例如，电池水平达到一定的阈值。

● 隐藏连接（承载和传输）建立和拆除 M2M 应用。

● 进行 M2M 设备或 M2M 网关的软件和固件升级。

除了作为一个设备管理服务器的 NREM，GREM 和 DREM 提供以下功能。

● GREM 充当一个设备管理客户端面对面 NREM，而且还作为一个设备管理代理面对面 D′设备或其他设备。网络管理代理允许 GREM 代替 NREM 执行设备管理客户端。

● DREM 作为 NREM 的一个设备管理客户端。

为了说明一个高层的 NREM 使用案例，图 5-4 提供了一个高层次的消息流，展示了 NREM 如何被用于设备管理。

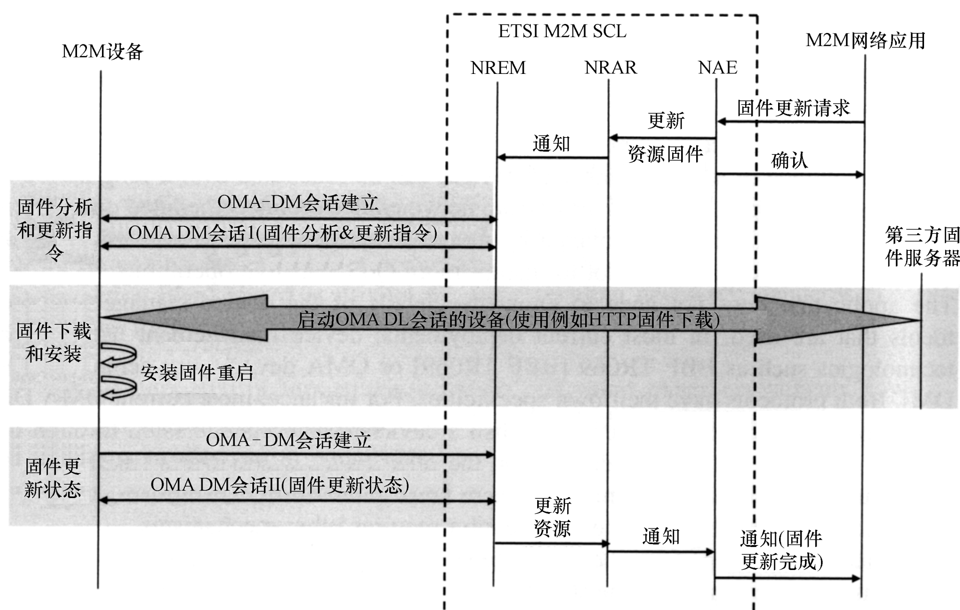


图 5-5　ETSI M2M 架构中升级设备固件的 NREM 使用

图 5-5 显示了 NREM 服务功能在满足 M2M NA 要求的情况下如何执行一个设备的固件升级。最初，M2M NA 请求一个固件更新。对于这样一个请求的参数必须包含一个设备订阅的标识符，以及固件映像的 URL 存储在一个服务器上（图 5-5“第三方固件服务器”）。这个请求将导致在 NRAR 中创建一种特殊的资源，包含固件升级操作的一个特定状态。NREM 会被通知需要进行固件升级。在这种情况下，OMA 设备管理被假定为管理协议，用于管理设备的生命周期。OMA DM 服务器请求建立 OMA DM 会话，它可以完成发送特定的消息或通过 HTTP 推送。这个会话将被用来传达 M2M 设备 DREM 服务功能对应固件升级的一套指令。这些包含其他部分，固件图像的 URL 以及需要接入该图像的凭据：用户名和密码。DREM 将下载固件图像，安装它，并开始重新启动。DREM 通过 DM 服务器建立会话，以便报告执行操作的状态，特别报告这些状态是否成功。如果成功，通过 NRAR 和 NAE 将一个确认传播到所有的 NA，NAE 代表网络域中 xAE 的实例化。

5.5.3 安全性能（xSEC）

该性能允许服务层登记——必要步骤，以允许设备或网关开始具有网络服务功能的操作。服务登记包括相互身份认证、授权和引导。下面提供了这些功能的高层次描述。然而，读者可参考第 5 章中对于 M2M 安全更深入的概述。

- 相互身份认证：为了一个设备或网关可以接入由 M2M 运营商管理的特定资源，需要首先执行身份验证。在 NSCL 方面，NSCL 是与 MAS 连接的服务功能，即具有接入用户订阅消息的服务器。特别是，当一个设备或网关希望以 M2M 运营商的核心架构（NSCL）注册，NSEC 包括来自 MAS 的认证材料和设备（或网关）的挑战，而在同时通过 NSCL 到 DSCL 或 GSCL 的认证提供足够的鉴别消息。因此，NSEC 可视为“认证”的认证、授权和计费（AAA）术语。认证材料生成一个永久的、可共享的密钥证书叫做“根钥”（见第 8 章）。作为这样一个相互认证过程的结果，一个对称会话的密钥可被互相允许并且在 xSEC（一方面是 NSEC，另一方面是 DSEC 或 GSEC）之间存储。会话密钥（或所谓的“服务密钥”）是用于进一步取得每个 M2M 应用的关键材料，这是为了在 mId 界面上创建安全数据连接的目的，以及为了应用层授权。注意，不同的 M2M 运营商可以配备不同类型的验证服务器。在一个特别的情况下，这些运营商希望重新使用他们现有的身份验证服务架构（如 HSS 或 AAA 服务器），他们也可以用于其他的服务类型，例如网络接入。在此情况下，NSEC 的实施需要考虑最常用部署的身份验证技术，以方便不同的身份验证协议。通常情况下，是否考虑某些身份验证框架是一个简单的任务，如可扩展的身份验证协议（EPA）。
- 授权：相互认证成功后，MAS 为 NSEC 提供授权消息。这些消息指定系统配置，在一个特定设备中特定的应用可以被接入。根据有关资料，并且结合会话密

钥，NSEC 为嵌入一个特殊用户设备的每个应用生成密钥凭据。这种材料是由 NSEC 填充到 NGC（网络域中 xGC 的实例化）且用于确定在 mId 界面上特定的 HTTP REST 命令是否可以被授权。注意，并不是所有由 NSEC 执行的操作对应由 GSEC 和 DSEC 执行的操作。例如，只有 NSEC 与 MAS 连接，在设备/网关中 DSEC/GSEC 与一个安全的环境连接，进行所有敏感的安全操作，例如充分利用根钥的关键推导函数。在另一方面，也有一定相似的功能，如从会话密钥而来的关键材料推导，这是用于在 mId 参考点建立 M2M 安全数据会话。

- 引导：在某些情况下，可以在用户订阅激活之前使用 NSEC，正如在第 8 章中讨论，服务引导程序允许设备/网关永久地与一个特定的 M2M 运营商的架构相关联，通过一个永久性的引导共享根钥以及其他服务参数和配置。在这种背景下，每当 NSCL 被认为促进根钥的自动引导时，设备/网关通过使用 NSCL 架构与 M2M 服务引导功能（MSBF）进行通信。鉴于 MSBF 可能是实体拥有和 M2M 服务运营的提供者，设备/网关需要先通过身份验证才能被授权，以达到 MSBF。这样一个（相互）身份验证是由 NSEC 再次执行。自动引导过程的例子在第 8 章中讨论，该过程利用了 xSEC 功能。

5.6　M2M 的 REST 架构格式简介

5.6.1　REST 简介

REST（表述性状态转移）是由 Roy T Fielding 在 2000 年［Fielding］中定义的一种架构格式。它是一套原则，支持分布式系统以实现更高的可扩展性，并允许分布式应用随着时间的推移发展和变化，这得益于组件之间的松散耦合和无交互状态。

REST 的主要概念是由资源组成的一个分布式应用，这些资源是嵌入一个或多个服务器中的消息的状态块。无论其内容如何，在 REST 中，通过一个统一的接口操作资源是可能的，这个接口由四种基本的相互作用组成：CREATE、UPDATE、DELETE 和 READ。这些操作中的每一个都是由请求和响应消息构成，除 CREATE 外，它们是等幂的，也就是说，不管其自身重复多少次操作，每个操作的最终结果是不变的。换句话说，这些操作没有副作用，这意味着它可以分配资源和使用代理功能。副作用的缺乏允许更有效地利用缓存和更大的可伸缩性。

然而，更重要的是，由于相同的一组操作可以操纵多种多样的资源，当应用域发生变化时，开发专用的客户端或架构是没有必要的。因此，相同的架构可以重复使用于多种应用。

最常见的 REST 实现是 HTTP，由此将 REST 操作映射为 HTTP 方法：CREATE

被映射到 HTTP POST，READ 被映射到 HTTP GET，UPDATE 被映射到 HTTP PUT，DELETE 被映射到 HTTP DELETE。

5.6.2 为何在 M2M 中使用 REST

如今，我们周围的许多设备包含越来越多的传感器。例子包括许多手机的 GPS 天线，包含在一些设备中的加速器、重量传感器（如用于电梯或游戏机），以及更传统的设备，例如烟雾、湿度或温度传感器。

传感器作为典型的设备，它可以将一个或多个典型的测量值转换成模拟或数字信号，例如数据处理和/或为驱动器提供输入。后者是采取某种输入形式的设备，并用它来执行物理作用的某种形式，例如关闭阀门或打开一盏灯。

传感器和驱动器往往连接在一起，通常使用计算设备的某种形式，将传感器的输出传送到驱动器的输入。这意味着，传感器和驱动器通常包含非常少的计算能力，而且它们是高端专用设备，限制它们自身的特定测量活动。随着时间的推移，配备有计算能力的微控制器，以及基于通信接口的标准已经出现，比如 WiFi、USB 或ZigBee。它们可能也提供一些机载遥感功能，比如 GPS 模块或加速器。这使得在进行测量和控制驱动器方面，允许一些更大程度的智能化。然而，它们的计算能力可能相差很大，尤其是因为许多设备是电池供电的，这意味着它们必须防止 CPU 不断消耗电池的电力。下面是具有传感功能的 M2M 设备的一些例子：

- Sun™ SPOT（见图 5-6）是一个 180MHz、带有 512KB RAM、4MB 闪存的 32 位 ARM920T 核心，且带有集成天线的 2.4GHz IEEE 802.15.4 无线电设备。它提供了一个 AT91 定时器芯片、一个 USB 接口和几个传感器，包括温度、光照和三轴加速度计。它可以支持外部模拟输入，并且可以通过 Java 编程。
- Sentilla™ JCreate 是一个 AAA 电池供电的微控制器，搭载了一个 TI MSP430 16 位微处理器和一个 TI/Chipcon ™ CC2420 无线收发器。它携有一个机载三轴加速度计和八个 LED 灯，并且它可以从第三方运行 Java/J2ME 软件。
- Crossbow™ TelosB 是一个带有 10KB RAM、IEEE 802.15.4 和 USB 接口的 TI MSP430 16 位微控制器，支持 Contiki、TinyOS、SOS 和 MantisOS 操作系统。通过 USB 可以接入/编程，并提供任选的机载温度、光照和湿度传感器。

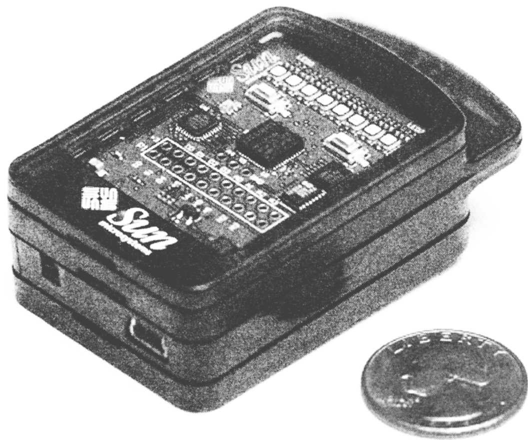


图 5-6 Sun SPOT M2M 设备

• Nano-RK FireFly™ 是一个带有 8KB RAM 和 128KB ROM 的 Atmel™ ATmega1281 8 位微控制器，ROM 带有 Chipcon™ CC2420 IEEE 802.15.4 标准兼容的无线收发器。任选的扩展卡可提供光照、温度、声音、被动式红外运动、双轴加速度和电压感测。

使用设备的这些实例应用对传感器通信的低层方面特别重视，如实时交互、能源消耗、纠错和硬件故障的管理。

另一方面，分布式系统开发的典型方法是在通信低层的顶端创建一个一致的抽象化（如使用 TCP/IP），并且在此之上定义交互模型。随着时间的推移，世界上已经出现了分布式系统的多种结构，例如 Java RMI、CORBA、DCOM 或 SOAP。其中大部分是基于以下假设：通信就像一个远程服务的调用，其性质可以忽略不计，因此可以考虑远程过程、远程函数或远程方法。这种方法被称为一个远程过程调用（RPC），而且这种方法假定通信范式总是涉及一个抽象的实体，这个实体发送一个请求，另一个发回一个响应，这两者通过一个可靠的信道进行传输。

传统上，分布式计算专家已接近使用相同 RPC 范式的传感器应用。然而，描述 RPC 的上述假设对 M2M 类型的应用并不总是适合的。

事实上，M2M 大多是实实在在的状态，模拟它们的技术与用于处理真实状态的一般程序方法相比更为适合。REST 是 M2M 模型的理想方法。REST 隐藏的概念是，每一个物理和/或逻辑实体是一种资源，这种资源有一个可以被“操纵”的特别的状态。这个概念很自然地映射到传感器领域和一般的 M2M 设备，一个传感器是一个可被读取或配置的设备，并且甚至可以向外界发送数据。

当然，没有什么能阻止传感器的建模或作为 web 服务和使用 WS-＊标准的 M2M 设备的全部范围。然而，这样的解决方案是非常复杂的，并且复杂性会带来消耗，这种消耗可以排除一大类资源受限的设备，特别是那些以最大渗透进入市场的设备。

基于 REST 的架构提供了多种优势，这些优势对传感器和 M2M 应用开发可能有用，例如通过一个 web 浏览器可视并控制传感器数据和校准参数的可能性，甚至使用一个或多个传感器或者作为数据源的 M2M 设备创建 web 混聚应用。

一个有利的结果是状态转移到客户端可以由浏览器和 HTTP 代理缓存，允许一个比任何基于 RPC 的方法更大的可扩展性，其中每个请求必须流向端到端。每一次通信是无状态的事实也增强了可扩展性，而且每个请求可以独立地进行处理。

传感器，一般的 M2M 设备和 M2M 应用从中受益颇多，因为它意味着一个具有缓存的简单的 HTTP 代理可以保护 M2M 设备（包括传感器）免受大多数网络负载。这是很重要的，因为事实上，大多数传感器设备是短暂的实体，它具有非常有限的处理能力。

最后，开发应用所需付出的努力大大降低，因为 REST 采用一种比大多数面向服务的体系结构（SOA）技术更轻的工具链。创建完全成熟的 M2M 应用需要简单的 HTML 和 Javascript。

采用 HTTP 的另一个副作用是传感器被当做 web 连接处理，可以发布在互联网上，包含在 RSS 集合内或通过电子邮件发送。

5.6.3 REST 基础

REST 是一种架构格式，在很大程度上依赖于 HTTP，并且将可接入的 web 资源的想法概念化。在 REST 条件下，一个资源可以是任何实体，可以用一个 HTTP URI 来解决（见图 5-7）。

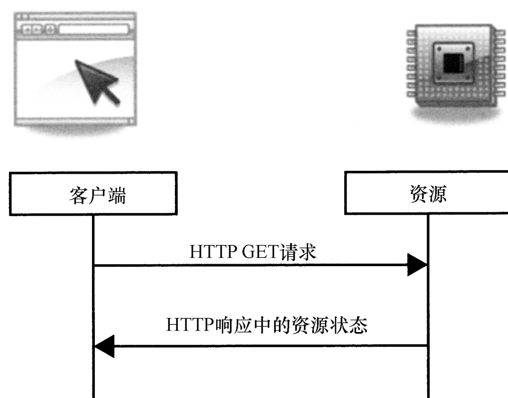


图 5-7 寻址一个 REST 资源

在 web 服务器中 URI 的主机、端口和路径部分被用来定位资源，并且在 HTTP 请求中使用 HTTP 方法确定采取什么样的功能。

HTTP GET 方法读取资源的“状态”并在 HTTP 响应中返回。在 REST 中，GET 方法被认为无副作用，这意味着在同一资源上多次重复相同的 GET 请求不会改变它的状态。

这也意味着，一个 GET 请求的传递在查询字符串中的任何参数只能影响到正被返回电流响应（由于过滤一部分或改变格式）。它不影响资源的远程状态。

HTTP GET 的响应也可以由客户端或通过任何中介代理缓存（见图 5-8），降低资源上的负载。

HTTP PUT 方法用于更新资源状态。利用这种机制来更新状态有几个优点，包括状态被设置在一个单一的功能中。这使得一个原子操作状态的编写只能成功或者失败，避免客户端和服务器之间的有效状态交互的需要。

此外，中间代理能够识别 URI，并随后快速清除其缓存。

还有另外两个 HTTP 方法，POST 和 DELETE，它们是非幂等性操作，通常分别用于创建和销毁资源。它们作为 PUT 以同样的方式工作，并且也是原子的。

由于原子，这种做法促进了 web 客户端和资源之间的“对话”方式，限制了副作用的数量，因为只有资源状态是被传输到资源或是来自资源，而不是功能。这就是处理传感器时所需要的。

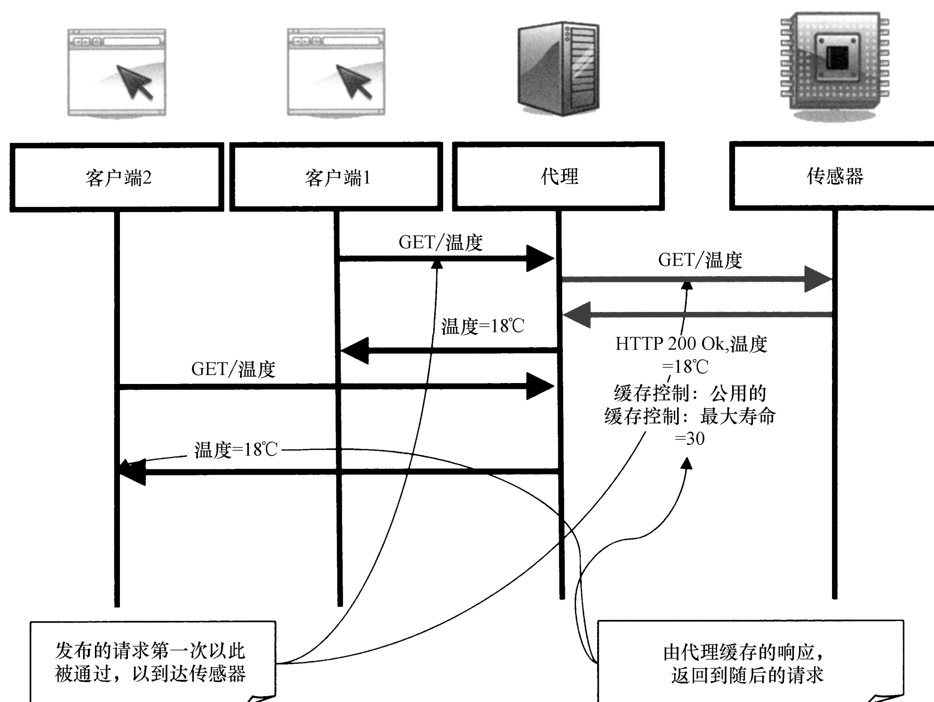


图 5-8　代理缓存的温度值

5.6.4　在 M2M 中应用 REST

M2M 设备间通信时如何使用 REST？

有多种方法可以用来实现有效的通信，根据一个事实，即一个物理设备被看做是一个资源，该资源可以通过一个 HTTP URI 接入，其样品可以使用 GET 读取并使用 PUT 校准。

POST 和 DELETE 与物理设备结合使用时可能看起来会很奇怪，因为这些既不能被创造也不能被消灭。然而，它们可以被用来配置更复杂的实体，如可编程滤波器。POST 可以被用来“添加”一个滤波器构成一组现有的滤波器，这些滤波器将被应用于一个处理传感器数据的计算装置。

传感器使用 HTTP 请求可以直接到达，并在响应消息中返回采样数据。这对那

些永存的设备非常适用，但是充分体现了它们潜在地巨大的流量。为了防止这一点，可以在客户端和传感器之间使用高速缓存代理。

如果一个传感器并不是永存的，它可能变得遥不可及。但是，在有些情况下，已知的最后一次抽样状态应该返回。

在这种情况下，资源不会成为传感器，但在一个 web 服务器中仅仅存在一个文档，该文档是带有最新样本数据的更新，当使用 PUT 时传感器需要最新样本数据（见图 5-9）。

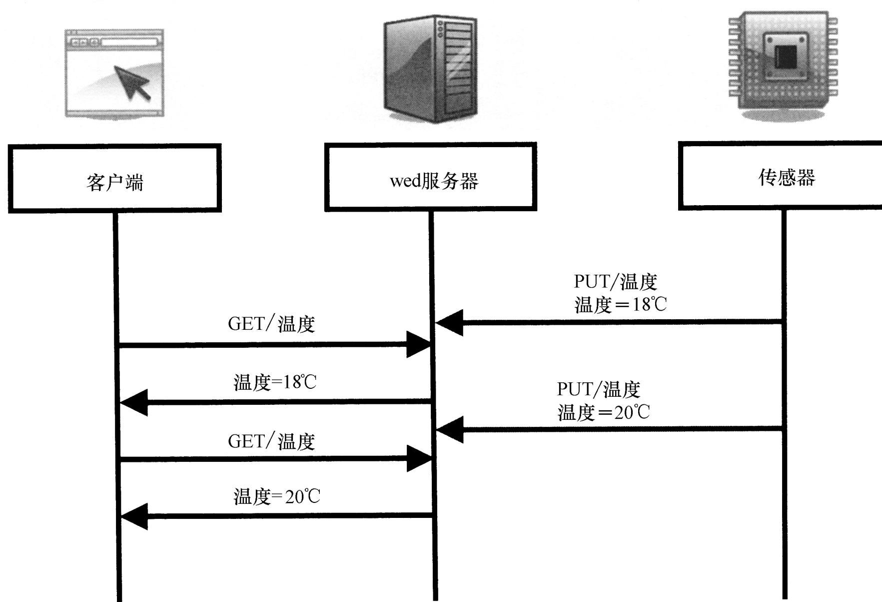


图 5-9　传感器使用 HTTP PUT 更新其采样

如果这是不可能的（例如如果一个传感器没有一个 IP 接口），有一个中间实体可能是必要的，它可以利用本机接口与传感器进行通信，以及与 web 服务器进行通信。这也可以包含在 web 服务器本身，因为许多服务器都可以承载第三方的应用，可以实现传感器的本地协议（见图 5-10）。

5.6.5　附加功能

5.6.5.1　事件处理

有些浏览器，几乎每一个可用的代理，支持“multipart/x-mixed-replace” MIME 类型。这种 MIME 类型允许响应以“块”被发送回客户端，每块取代以前的一个。这种技术被称为“服务器推”，被用来强制一个 HTTP 服务器执行连接的客户端在 web 网页上所显示的变化。这种技术通常利用网络摄像头来更新它们正在生

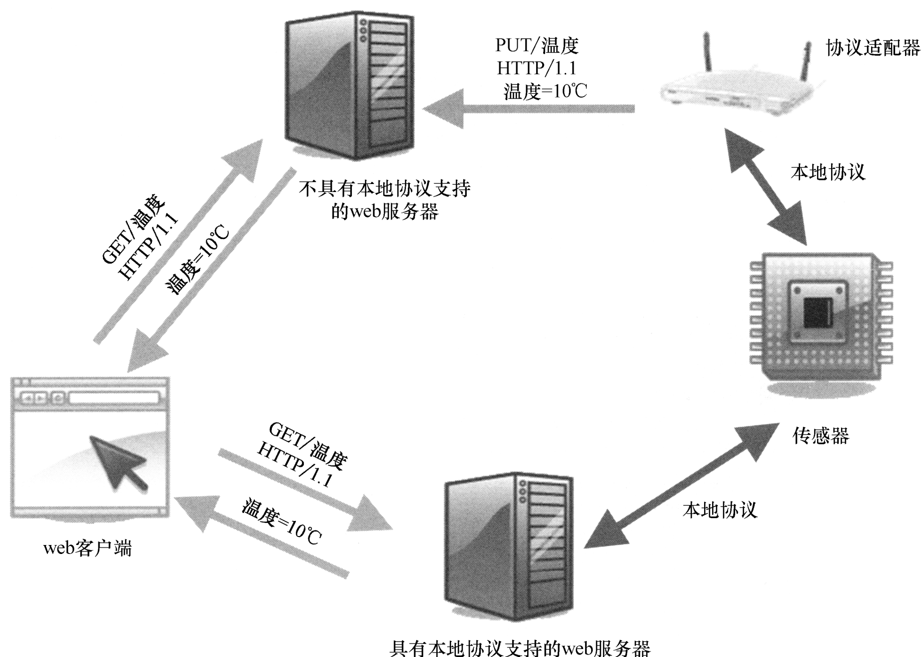


图 5-10　使用本地协议连接传感器

成的图片。

传感器可以使用这种技术在流媒体方式中提供样品给连接的客户端。当一个传感器产生一个新的样本，每个连接的客户端将收到 multipart 响应的一个块。这允许异步事件被传递到客户端（见图 5-11）。

服务器推送技术的一个主要缺点是，一个 TCP 连接需要对客户端订阅样品事件的整个过程保持开放，严重影响到可扩展性。但是，使用 HTTP 代理可以在很大程度上缓解这个问题。它可以减少一个传感器到另一个传感器的直接连接的数量，每当客户端订阅事件流时它由代理服务器制造。代替连接到传感器，客户端将连接到代理服务器，其能够服务于多个连接。

另一种 HTTP 技术可以使传感器将事件发送 HTTP 长轮询（见图 5-12）。根据该技术，客户端连接到资源并在一个 TCP 连接上发送一个请求，然后它等待一个到达的响应。受到质疑的 HTTP 请求中的传感器，在一个新的样本可用之前，它会使客户端等待 TCP 连接，然后将它作为一个 HTTP 响应发送回来。收到样品后，客户端将发出一个新的 HTTP 请求，以等待下一个样品的产生。

在这种情况下，连接被保持打开的时间周期是相当长的，这意味着资源消耗与

先前的机制是非常相似的（见图 5-11）。然而，该技术是浏览器和代理更加友好型的技术，因为没有必要支持特殊的 MIME 类型，并且传感器/M2M 设备只是模拟一个非常缓慢的 web 服务器。然而，multipart 情况的优化考虑仍然适用。事实上，它能够使用一个或多个代理，以便多路复用 HTTP 响应对应几个连接的客户端，这些客户端为实际的传感器/M2M 设备使用一个单一的连接。

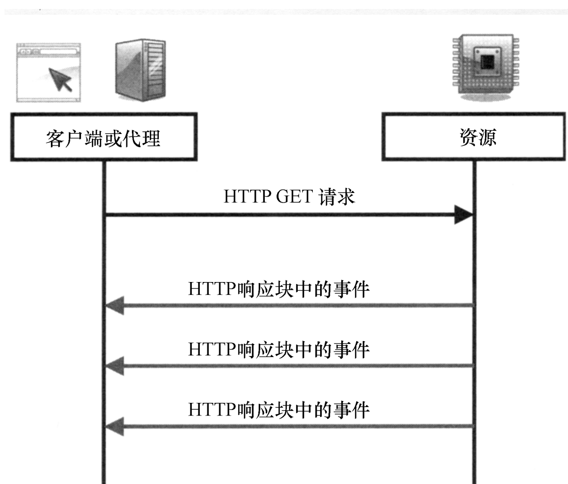


图 5-11 相同 HTTP 响应中的多个事件流

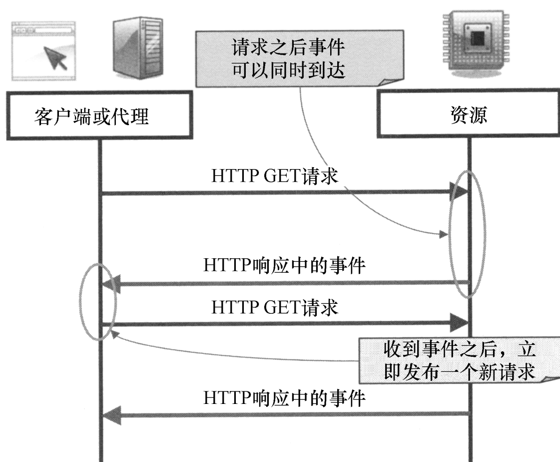


图 5-12 作为 HTTP 请求被发送的事件并且为了接收下一个事件发布一个新请求

5.6.5.2　通过使用高速缓存代理提高效率

传感器采样数据的缓存以透明的方式可以提高整体系统的可扩展性。透明度通过高速缓存只要求普通 HTTP 代理的引入得到确保。从传感器和它们的客户端的观点来看没有明显的变化。修改后的拓扑图可以成为一个更大的请求数。高速缓存控制以同样的方式与正常的 web 浏览存在。一种方法是使用请求中的“If-Modified-Since”HTTP 报头。事实上，在 GET 请求的响应中使用 HTTP“Last-Modified”报头，一个传感器可以返回其最后的采样的实际时间。客户端和/或每一个中间代理保留此值，可以将它放在每个后续请求的“If-Modified-Since”报头中。

如果没有新的样品，传感器对这些请求只是简单地返回一个 HTTP 代码 304（未修改），“Last-Modified”报头包含最后一个样品的时间。

在客户端和服务器之间的一个代理检查所有过往的流量，并注意多个传感器的最新样本数据。当一个 GET 请求到达一个客户端，并将它传递到传感器，如果返回 304 代码，那么即使客户端不指定其请求中的“If-Modified-Since”报头，代理也不会返回最后一个已知的样品。

此外，在请求和响应中使用“Cache-Control”报头，传感器、客户端和代理服务器能够以更复杂的方式控制资源的缓存（见图 5-13）。除了那些已经被 HTTP 协议预见的指令，它也可以指定新的缓存指令。它是可能的，例如，一个传感器通知被返回样品时间有效性响应的收件人（无论是客户或代理），以及在样品的验证期

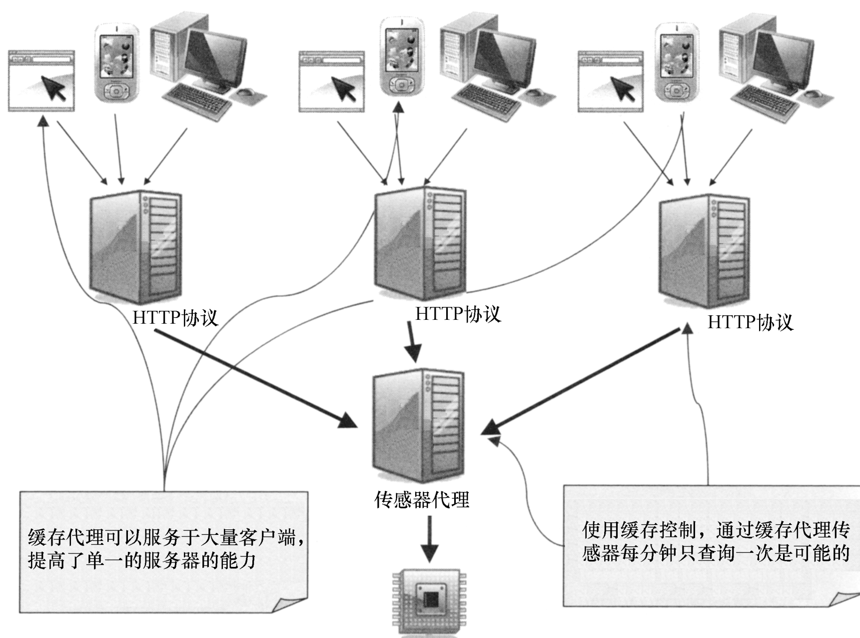


图 5-13　使用缓存代理提高可伸缩性

满之前是否需要重新生效。

在过期之前，这种机制通过代理被用于为客户端返回最后一个已知的样品，到期之前没有接触到传感器。

高速缓存极大地降低了传感器的通信量，因为电流采样到期后只有一个请求被发送给它，并且直到新的到期没有发送进一步的请求。

5.6.5.3 设备配置示例

设备要做的不仅仅是由测量产生数据。它们还需要进行配置和校准。例如，需要一次又一次的校准激光计，以调整其内部硬件的测量参数。当校准发生时，一些有关物理大小的参考消息被发送到正在执行样品测量的传感器，并且样品和参数之间的差异通过传感器被用于对准其进一步的抽样。另一方面，当传感器没有执行样品测量时，配置也可以用（在某些情况下，这是必须的），并且它涉及发送传感器关于如何进行操作和/或通信的必要消息。

在所有这些情况下，有必要发送传感器的一些校准或配置数据。在 REST 中，以下三种方法本质上是可能的。

第一种方法允许传感器配置数据被直接发送到使用 HTTP PUT 或 POST 方法的传感器。然而，这是唯一可能的，如果传感器本身可以由 HTTP 编址，对不永存设备或设备不支持 IP 连接时，这种情况是不存在的。

在这种情况下，在客户端应用和传感器之间必须有一个 HTTP 代理，此处的传感器能够将接收的数据从 HTTP POST 请求转换成一组传感器命令。然后这些命令作为 POST 请求的一个结果被立即发送到传感器（见图 5-14）。

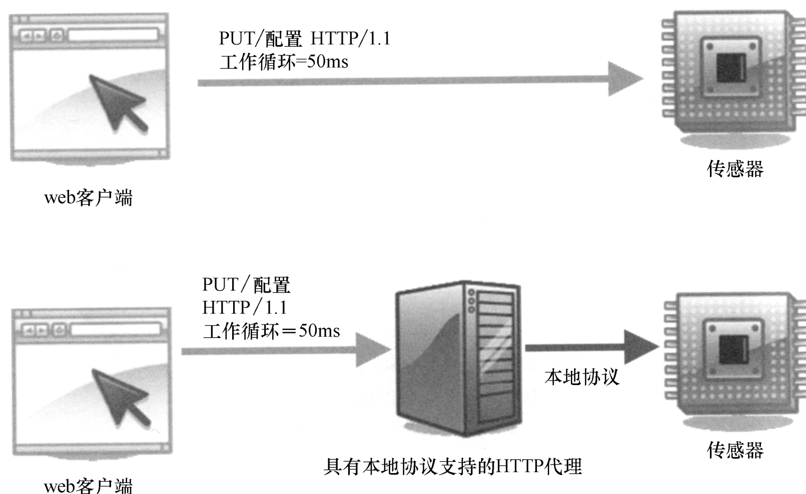


图 5-14 直接配置或具有代理的传感器

然而，当传感器并不永存时，有必要通过 HTTP 代理存储的一个应用发布配置数据，该代理包含一个高速缓存或存储库，并且当它在网络运行时由传感器获取，如图 5-15 所示。最后，检索这些消息可以采取两种方式进行：如果不支持 IP 连接，传感器可能发出一个 HTTP GET 请求到代理或使用其本地协议。在后一种情况中，代理也必须支持此协议。

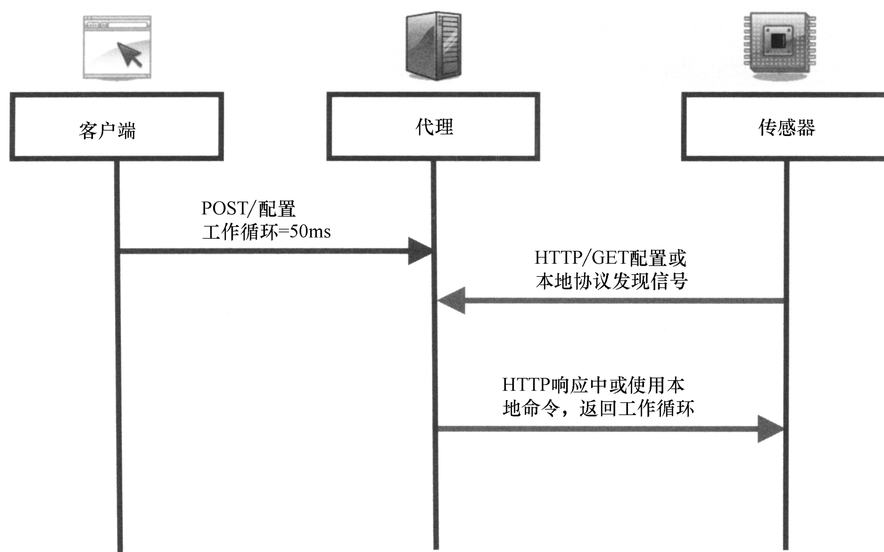


图 5-15　使用 HTTP 代理的异步配置

5.6.5.4　REST 附加功能

REST 的另一个特点是，它可以为每一个设备选择 URL，为了揭示其状态，可能要使用该 URL。使用其环境路径部分将状态进行编址，通过使用一个 HTTP URL 这是可以做到的。对于复杂的系统，使用不同的 URL 以存储不同子系统的状态，这也是可能的。

例如，“智能” 汽车的部分状态被公开在一些 URL 上：

- http：//carmaker. com/numberplates/00001/wheels。
- http：//carmaker. com/numberplates/00001/engine。
- http：//carmaker. com/numberplates/00001/battery。

应该指出，当一个资源被创建时，资源的 URL 有时是动态地生成的。这通常发生在使用 POST-Redirect-GET 范例创建资源时。在这种模式下，设备通过创建一个资源第一次公开其状态，该资源将 HTTP POST 用作一个预定义的 URL。在另一个 URL 内创建资源，此 URL 被返回包含 HTTP 响应的设备（见图 5-16）。

新创建的 URL 可以通过使用 HTTP PUT，由设备被用于更新其状态（见

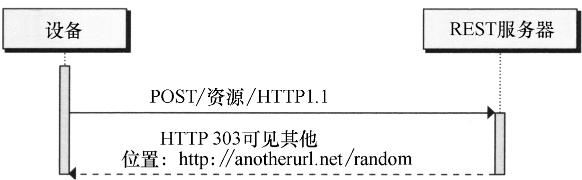


图 5-16　设备方面的资源创建

图 5-17）。

即使它是脱机的，其他设备可以使用该 URL，以便检索设备的状态。为了使这些设备检索动态生成的 URL，在一个发现服务器中存储该 URL，例如，在 DNS TXT 记录中具有 DNS-SD。由于公布是长期存在的（它可以一直存在，直到底层的 M2M 设备得到配置为止），入口停驻的时间比典型的设备唤醒时间更长（见图 5-18）。

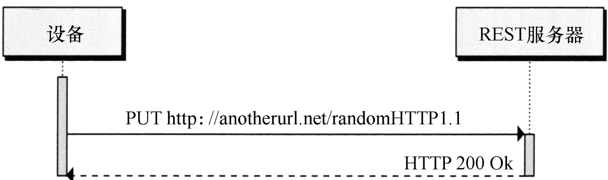


图 5-17　根据其当前状态设备更新一个资源

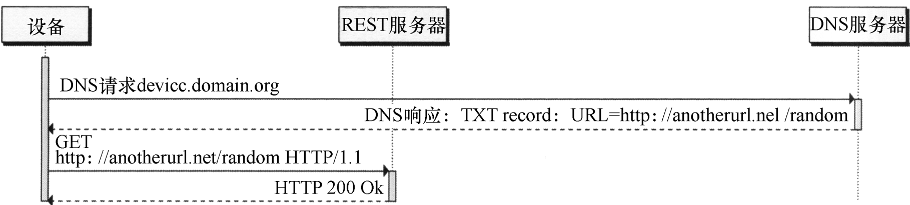


图 5-18　DNS 查询检索一个设备状态的 URL

通过这种方法，对消息的接入控制变得容易，作为设备制造商或系统管理员不必考虑他们的设备如何验证其他设备和用户，只考虑连接的设备和 REST/HTTP 服务器。例如，是否需要具有 DNSSEC 和 HTTPS 服务器的认证，这是可以做到的。REST/HTTP 服务器管理员必须验证设备，所以只有特定的设备可以写入到特定的地址。基于 TLS（传输层安全）这也是可以做到的。

5.6.5.5　与其他标准的关系

1. IETF CoAP

作为 6LoWPAN（IPv6 的有损压缩和低功耗的 PAN）的一个扩展的概念，

CoAP[一] 是 IETF 围绕的另一个基于 REST 架构移植到无线传感器网络的特点，特别是支持 6LoWPAN 的网络。基于 REST 架构定义了四个基本的操作，这些操作在处理资源（这种情况下的设备）时是可用的。这些操作包括创建，读取，更新和删除。使用这些操作的所有 REST 资源可能被操纵。一般情况下，REST 服务器使用 HTTP 作为传输，并且以上操作映射到 HTTP 方法分别是 POST、GET、PUT 和DELETE。

CoAP 提出的内容对 RESI 来说是一个非 HTTP 方法。这样做的原因主要是，在小的、有限的设备如那些 6LoWPAN 中，实现 HTTP 是有困难的。因此，CoAP 定义了一些原语，允许 REST 置于 TCP 和/或 UDP 之上。

为了简化消息格式，HTTP 报头已被简化为固定位置，固定大小的二进制字段，该字段包含 CoAP 载荷，并且只有一组有限的 MIMR 类型可用。

然而，即使有这些限制，在网络中创建网桥还是可能的，该网络可在 CoAP 和 HTTP/REST 之间做一个适当的转换（见图 5-19）。这允许有限传感器设备和 web 服务器之间更多的无缝集成。

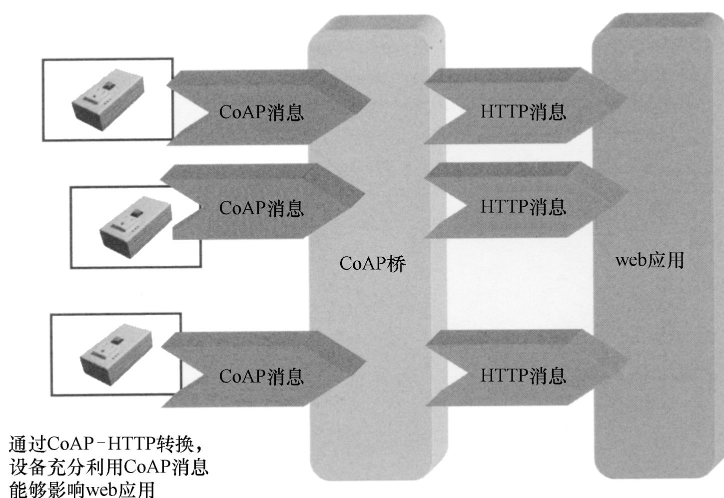


图 5-19　CoAP 到 HTTP 协议桥允许在设备和 web 应用之间无缝集成

2. SOAP

由于 REST 是一种架构格式，它不强加 HTTP 作为一种协议。如果底层协议能被重新改编成资源式的操作技术，然后用它们代替HTTP是可能的。例如，这是

[一] COAP(限制性应用协议）是由 IETF 指定的一种应用性协议。COAP 是一个基于 UDP（用户数据包协议）框架上运行的 Restfull 协议，特别适用于设备受限的网络通信中。

RESTful web 服务的情况。在这种情况下，一个设备可以充分体现一个 SOAP[1] 接口，该接口包含适当的 GetXXX 和 SetXXX 方法，这些方法可用于操纵其作为资源的内部状态（见图 5-20）。

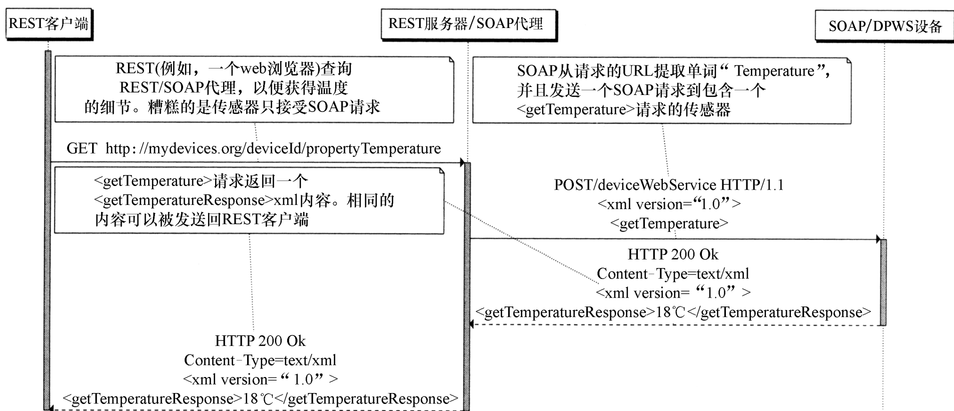


图 5-20　REST 到 SOAP 的转换

类似的方法能够使网关在没有更多重新适应的情况下支持多种协议。事实上，将 GetXXX 方法转换成 HTTP GET 请求现在已成为可能。

实际情况是，一个 SOAP 请求可以用 URL 的最后部分很容易地合成，这表明我们对资源的部分状态感兴趣。SOAP 响应在 HTTP 响应中作为 XML 片段得到通过。

这个机制能被用来充分体现 web 服务设备的设备外形和作为 REST 资源的后端 web 服务。

然而，应该注意的是，基于 REST 的系统和基于 SOAP 的系统之间有一个本质的区别。

事实上，REST 原则规定通过操作系统的接口必须是均匀的。这意味着以上描述的相同的 HTTP 方法对每一个 REST 资源都是相同的。

这种均匀性在 SOAP 和它的相关标准中是不存在的，因为对不同的 web 服务器（并且对不同的 SOAP 曝光设备）表现明显不同的接口是非常可能的。

为了弥补不同的 SOAP 系统之间的差距，有必要采用复杂和繁重的框架，如 J2EE[2]，每当一个新接口添加到该系统时，在额外的编程代价上为 SOAP 接口生成

---

[1] SOAP（简单对象接入协议）是一个基于 XML 的简单协议，该协议允许应用通过使用 RPC 在 HTTP 上交换信息。

[2] J2EE（Java 2 企业版）是一个针对企业应用而推出的 Java 规范标准软件平台。

编程语言绑定是可能的。

这意味着，当涉及的接口数量增加时（作为每个不同的设备类型提供它自己的接口的 M2M 中将会发生），系统的复杂性和开发成本将同样增加。

特别是，为服务新设备而扩展系统变得困难，当这些新设备在市场上流通时，它们的接口需要得到支持。

考虑下面一个温度计的例子，它可以读取一个房间的温度。通过 SOAP 接入它需要以下步骤：

1）温度计供应商应该公布（通常在一个 UDDI[㊀]库）温度计的 SOAP 接口。

2）程序开发人员希望在它的应用程序中包括温度，该应用程序下载接口描述（通常是一个 web 服务描述语言（WSDL）寿命），并且用 WSDL 启用技术编译它，例如，J2EE。这将在应用程序和用于编译 WSDL 的技术之间创建一种依赖关系。因此，如果一个应用程序的不同部分在不同的技术上得到实现，有必要为复杂技术的任何形式重新编译 WSDL。

3）生成的代码必须被集成到应用程序中。

对于任何原因，如果温度计的接口将来在某个点上发生改变，整个应用程序将需要被重建。

用 REST 代替使得事情更简单。事实上，用一个 HEEP GET 可以实现一个温度计的读取。

温度计客户端将指定首选的 MIME 格式（HTTP 接受报头）、编码（HTTP 接受编码报头）和字符集（HTTP 接受字符集报头），并且 M2M 服务器必须通过温度计将提供的数据转换成需要的那一个。

大多数 MIME 格式、编码和字符集是已知的，并且通过不同的应用程序实现转换的代码可以被重复使用，这是毫无疑问的。

例如，温度计客户端可以请求 M2M 服务器将温度采样作为一个音频/mp3 MIME 格式返回，而温度计将其样本作为一个纯文本返回。

5.7　ETSI TC M2M 基于资源的 M2M 通信及规程

5.7.1　引言

本节对 RESTful 格式如何适用于 ETSI TC M2M 架构提供了更深入的看法。在 ETSI TC M2M 中，定义在 M2M 架构上的所有三个规范性参考点都是假设的，即

㊀ UDDI（通用描述发现和集成服务）是一种基于 XML 目录服务的规范。

mIa、mId 和 dIa 将会使用 REST，尽管可能有一些例外。例如，在 mId 参考点上，使用现有的协议如基于 RPC 的 BBF TR069 和 OMA DM 进行设备管理。

ETSI TC M2M 没有假设 HTTP 会成为用于执行的协议，尽管在 CoAP（更适用于受限的设备）成为广泛部署之前，HTTP 是自然的选择。为了避免使用特定的 HTTP 原语，本节将主要使用四个原语。

- 创建：创建一个资源。
- 检索：读取资源的内容。
- 更新：编写资源的内容。
- 删除：删除资源。

这些方法被称为下面的 CRUD 方法。除了这些基本的方法，对资源改变订阅（S），以及对包括在一个更普遍的 RESTful 架构中的有关资源改变通知（N）而定义的方法通常也是有用的。假定如下的 CRUD 和 SN 适用于在 SCL（服务功能层）中所使用的资源。

图 5-21（源自 ETSI TC M2M TS 102 690）给出了一个用 REST 如何在设备应用和网络应用之间进行数据交换的例子。

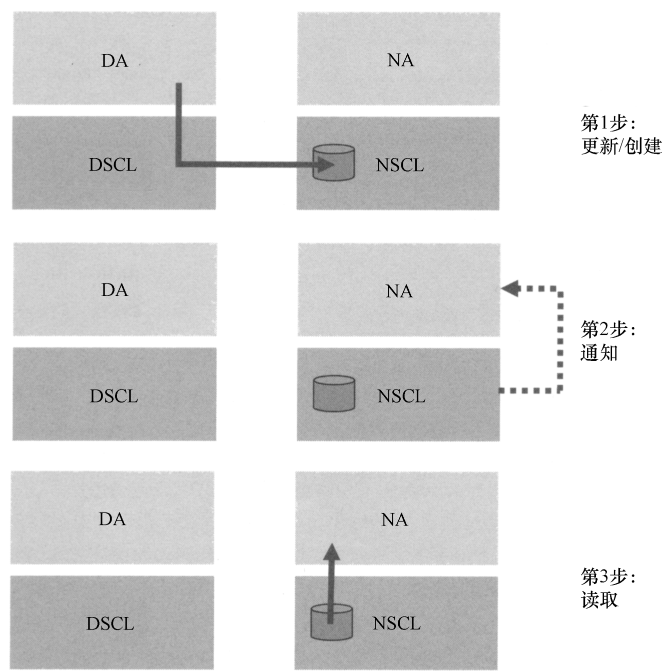


图 5-21 数据交换的 SCL 和 REST 架构格式的使用
（来源：ETSI TS 102 690）

图 5-21 中，第 1 步显示了 DA 如何请求在 NSCL（网络服务功能层）下存储的

特定数据。由于 DA 不直接与 NSCL 进行对话，所以在这种情况下，在 NSCL 下由本地的 SCL（即 DSCL）存储该数据是很容易的。DA 可以为此端使用一个更新或者一个原始的创建。

第 2 步中，NSCL 通知可用的一些数据，这是可以选择的。此步骤假定当数据与一个特定的标准匹配变得可用时 NA 已经同意被通知。第 3 步由通过 NA 获得的读取数据组成。

5.7.2　在本节中使用的定义

以下是在本节中使用的其他定义。这些定义与在 ETSI TS 102 690 中提供的那些是均衡的。

- 发行者：参与者执行一个请求。发行者可以是一个应用或 SCL。
- 托管 SCL：地址（主/原始）资源属于 SCL。
- 本地 SCL：SCL 的应用或 SCL 将会注册。它是第一个从请求的原始发行者接收到请求的 SCL（无论是一个应用还是一个 SCL）。
- 发布资源：该资源的内容是指由托管 SCL（主/原始资源）托管的资源。发布资源是一种包括只有一组有限属性（通常存储资源本身的消息，例如 lastModifiedTime）的资源，最重要的是搜索字符串，并连接到原始资源。此资源的目的是促进原始资源的发现，以至于该发现的发行者不必为了找到特定的资源而附属所有的 SCL。
- 公布的 SCL：SCL 包含公布的资源。一个资源可以被公布到多个 SCL。
- 接收器：从发行者接收到请求的参与者。一个接收器是一个 SCL 或一个应用。

5.7.3　资源结构

5.7.3.1　为什么要定义一个资源结构？

M2M 服务功能目的在于提供数据调解功能。在 TS 102 690 中 ETSI TC M2M 定义了一个具有树表示法的资源结构：

- 提供 M2M 应用，为数据调解功能使用 M2M SC，这是一种解决资源的有意义的方式。然而，就创建新的资源（特别是数据交换）而言提供了极大的灵活性。因此，数据结构并不意味着打破了去耦客户端和服务器的 REST 原则，而是提供了一个最小的方法，简化了解决方案（URL 建设），并且便于维护和数据生命周期相关的行动。举个例子来说，这种情况下当设备不再被登记时，在网络 SCL 上存储 DA 数据。如果其所有相关的数据很容易识别，那么从网络 SCL 移动它是很容易的。
- 描述资源的不同格式如何与其他的每一个相关。

● 使用最低限度的结构化数据来提高整个系统的性能。例如，假设有一个请求发现运行在一个特定的设备上的所有应用——使用一个 URL 更容易，其中运行在一个给定的设备上的所有应用有一个表示。

5.7.3.2　用于资源结构的资源格式

图 5-22 提供了一个在 TS 102 690 中指定的资源树结构的概述。为了提供此资源结构的概述，下一节将提供用于资源结构中的一系列资源格式。一个特定的资源格式通常被用于不同的资源，该资源是资源树结构的一部分。

● sclBase 对于由 M2M SCL 托管的所有其他资源是根源。sclBase 资源由一个绝对的 URI 编址。在 sclBase 下的所有其他资源将会有一个 URI，该 URI 从 sclBase 的 URI 分层派生而来。例如，一个特定的 sclBase 资源识别一个通过 URI：<protocol>：//m2m. operator. com/编址的网络 SCL。一个存储器资源（用于数据交换的特定资源）的 URI 例子由相同的 SCL 托管：<protocol>：//m2m. operator. com/containers/meterDataSamples/。

● scl 资源代表 M2M SCL 管理其他实体。对于 sclBase 对应的一个 NSCL，scl 资源允许在 DSCL 和 GSCL 上与 NSCL 相互注册的信息的存储。注册（因此一个适当的 scl 资源的存在）为了交换数据对于 SCL 来说是一个先决条件。注册的 scl 资源将包含其他资源，例如，提供注册在远程 scl 上的应用的一个局部表示。

● 应用资源存储关于应用的消息。应用资源作为一个应用的成功注册结果得到创建。应用仅仅注册到其本地的 SCL，但是对于已经注册的本地 SCL 而言 sclBase 是已知的。

● 存储器资源是一般的资源，通过使用作为一个负责缓冲数据的调解员的 M2M SCL，被用于交换应用和/或 M2M SCL 之间的数据。

● 接入权限资源存储一个认可的表示，该认可有资格为资源树结构的部分接入管理实体。接入权资源在 SCL 下被连接到其他资源。

● 组资源存储一组其他资源的消息。组资源的优点是它允许发行者，例如一个应用，当其想发送数据到一系列接收器时只写一次，从而简化了 API 上的交互。在这种情况下，SCL 可能需要将数据转载到组成员的资源上。

● 订阅资源对其父资源记录主动订阅的状态。当一个特定的事件发生时，订阅允许通知订阅者，例如，在资源上执行的更新。

● 在 ETSI M2M 中使用采集资源是为了允许具有一定共性的资源分组在一起。采集中的分组资源为每个发行者提供一个方法，以便使用单独的 URI 引用一组资源。ETSI M2M 资源树结构在不同地方使用采集，例如，SCL、应用或存储器。

● 发布资源是一个特定的资源，其中包含有限的一组属性，例如一个搜索和一个到原始资源的连接（URI）。通常在远程 SCL 中，允许发布资源由资源的部分表示，以便允许发现（特别是充分利用搜索属性）而无需查询 SCL 托管。只有当发

布资源通过其完整的 URI 直接接入时，它是可见的。

● 发现资源是一个用于允许发现的特定资源。它被用来检索一系列与一个发现筛选标准匹配的资源的 URI。

5.7.3.3　ETSI M2M 树结构模型

图 5-22 为资源提供了一个树结构：一个资源的逻辑分组允许资源的简单寻址、交换应用数据的灵活性和简单的 API。使用以下符号：

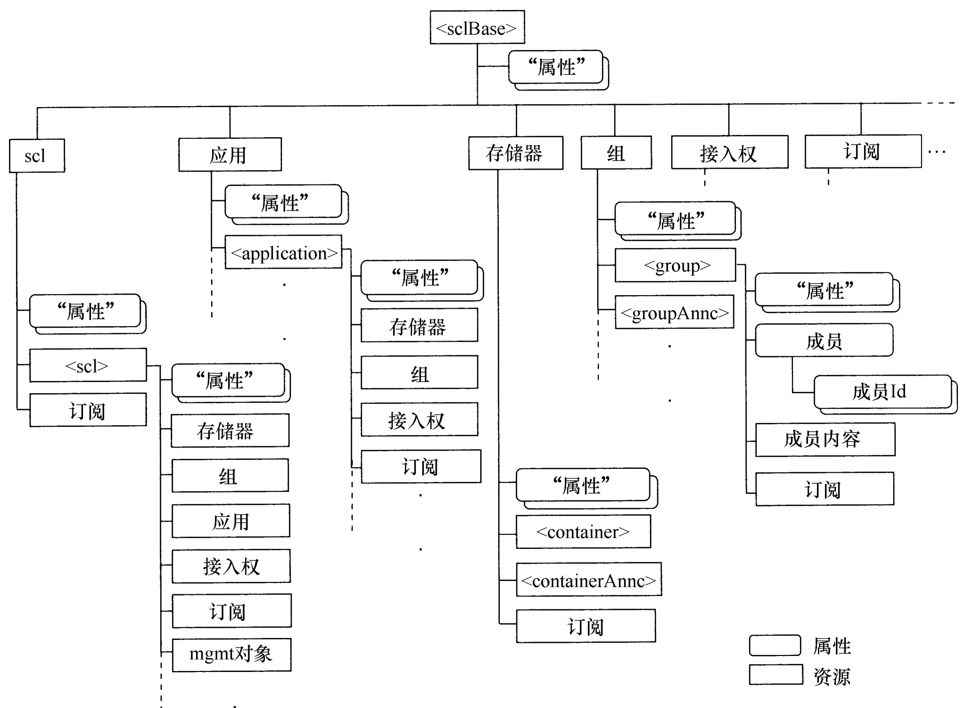


图 5-22　ETSI TC M2M 资源结构（由 ETSI 许可转载）

● 符号 < resourceName > 意味着一个特定格式的资源名称的占位符。资源的实际名称不是预先确定的。在实践中，它可以通过 SCL 动态地进行分配或者通过资源的创建由发行者来选择。例如，应用收集资源下的 < application > 资源的例子，它的实际价值可能是“utility 1 smartmeterApplication”。在这个例子中，根据图 5-22 中的资源结构，每一个应用的 URI 可能是：< protocol >：//m2m. operator. com/applications/utility 1 smartmeterApplication/。假设 < sclBase > 是 < protocol >：//m2m. operator. com/，其中的 < protocol > 是用于接入资源的实际协议。ETSI M2M R1 已经选择 HTTP 和 CoAP 作为用于实施的两种可能的协议。

● 当分隔符“ < ”和“ > ”或“..”不被使用时，对于固定的资源名称，出现在方框中的名称是文字。

● 方框用于资源和子资源。

● 圆框用于属性。属性存储有关资源本身的消息，例如 lastModifiedTime。属性可以是强制的或是任选的，且有读/写权限。属性以完全相同的方式被编址为资源。例如，如果发行者想读取有关最新接入的 sclBase 消息，它需要使用 URI 来发行一个原始的读取：<protocol>：//m2m. operator. com/lastModifiedTime。

● 所有采集资源总是复数形式（以“s”结尾的名称）。采集资源与其子资源之间的基数由“<”和“>”分割，且一直是复数。

图 5-22 提供了树结构的部分表示，其中可以得出以下结论：

● scl 资源是资源的一种采集。对每一个已注册的 SCL，为了记录 SCL 与本地 SCL 有关系，创建了一个 <scl> 子资源。其他 scl 的子资源是订阅，这是一个采集，为资源 scl 提供了一个订阅的表示（例如，发行者，时延容限等）。<scl>包含多个子资源，例如应用是所有应用的一个采集，这些应用都是本地集合订阅的 SCL。<scl>还包含一个存储器采集，这是非常基本的资源，应用可以为交换数据创建存储器。存储器也可以在 <application>下创建。根据它们的业务逻辑，也根据存储在存储器资源下的数据寿命，使用一个或其他存储器资源的决定是应用本身的选择。

为了替读者简化大图，这是一个如何使用 scl 资源的例子。假设一个公用公司后端的计量应用使用 sclBase：<protocol>：//m2m. opterator. com/utility 1/。在 scl 采集下为每个注册的计量创建一个 <scl> 例子，URI：<protocol>：//m2m. operator. com/utility 1/scls/meter123456。假设一个智能计量运行两个应用，一个用于记录智能计量数据，另一个用于归属自动化。对于每个应用，创建一个 <application>资源实例（已公布的资源包含原始资源的一个有限的表示），并且这些通过 <protocol>：//m2m. operator. com/utility 1/scls/meter12345/applications/meter12345/和 <protocol>：//m2m. ooperator. com/utility 1/scls/meter12345/applications/homeAutomationApp12345/得到编址。假设，智能计量上运行的智能计量应用在 NSCL 下被配置为记录计量数据，报告数据的一个方法是在 <application>公布资源的一个存储器采集下将它存储：<protocol>：//m2m. operator. com/utility 1/scls/meter 12345/meteringApp/applications/meteringApp12345/containers/meterSamples/contentInstances/Day 1 H 1/。

● 应用采集资源被用于存储有关本地注册的应用资源（NSCL 的 NA，DSCL 或 GSCL 的 DA 和 GSCL 的 GA）。

● 接入权采集资源允许 <application>实例在一个单独的资源下被分组。一个 <accessRight>资源允许接入存储权限，也就是“允许”特定的接入模型的实体（permissionFlags：只读、读写、一次写入等）。图 5-23 中表示了一个接入权的资源结构，使用权限允许为实体存储 RIGHTS，这些实体连接到这个 <accessRight>

可以接入资源，而自身允许存储实体的权限，允许这些实体改变自身的接入权资源。作为一个建立在之前计量例子上的例子，假设接入权资源：<protocol>：//m2m. operator. com/utility 1/accessRights/smart metersRight/。为接入计量数据只允许计量后端应用配置此接入权限是可能的。所有计量应用资源需要连接到接入权资源的后端，以便只给实用的后端应用接入该数据。

表 5-1 提供了一个一些 REST TC M2M TS 102 690 常用属性的列表。

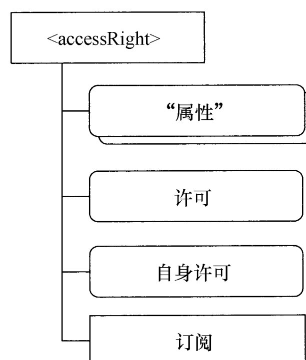


图 5-23　<accessRight>资源结构

表 5-1　M2M 一般属性

名　　称	描　　述
accessRightID	一个接入权资源的 URI。接入权资源中定义的许可，即确定谁可以接入该资源，该资源包含特定目的的属性（检索，更新，删除，等等）
creation Time	资源创建的时间
expiration Time	由托管 SCL 删除资源之后的绝对时间
last Modified Time	资源的最后修改时间
search String	用于发现资源的关键字

5.7.4　接口程序

接口程序在允许资源处理的 mIa、dIa 和 mId 接口上定义了一组原语和交互。接口程序的最终目标是允许 M2M 系统中的应用之间交换数据。然而，当完成一定数量的步骤时数据交换才能发生：

- SCL 发现定义了允许一个 DSCL 或 GSCL 发现一个 NSCL 的程序，以便进行登记。SCL 发现程序在本书出版的时候还没有被定义。ETSI M2M 架构的初始部署可以依靠配置。
- 一旦执行发现，SCL 注册允许一个 DSCL 或 GSCL 的程序注册一个 NSCL。SCL 登记对允许 SCL 启动资源管理程序是一个必要的程序。SCL 注册假设 SCL 进行适当的身份验证和授权机制，如第 8 章中描述的。
- 应用注册定义了一组允许一个应用注册到其本地 SCL 的程序。应用注册对一个已知的应用和使用基于资源的程序开始交换数据而言是必要的步骤。

一旦这些程序已经完成，SCL 可以执行任何以下应用要求的程序。

- 接入权限管理包含操纵（创建，删除，更新，检索）资源附属到接入权限。

• 存储器管理包含程序，该程序允许通过特定资源的使用进行应用数据交换，作为存储器资源被提及。

• 组管理包含资源的操纵组。组资源允许应用和 SCL 之间以及 SCL 之内平滑的相互作用。

• 资源发现允许资源发现存储在一个特定的 SCL 上，或资源通过过滤器标准的使用发表在 SCL 上。过滤器标准可能包含属性的组合，例如 creationTime 和 searchString。

• 采集管理定义了一系列程序来管理采集资源。

• 订阅管理定义了一组程序，当特定的订阅标准得到匹配时，允许应用或 SCL 订阅和通知。

• 资源公布/解公布程序定义了一组程序，允许资源被公布和解公布到一个远程 SCL。

通过一个具体的例子更好地解释了接口程序。然而，这个例子将不会提供所有定义在 TS 102 690 中可能的程序。

5.7.4.1 通过一个例子进行资源管理：智能计量

在这个例子中，做了以下假设：

• NA 是一个智能计量应用，该应用已经与通过一个 M2M 服务提供者经营的 NSCL 注册：两个实体之间达成的 <sclBase> 是：<protocol>：//smartmetering. utility 1. com/。

• 一个特定的智能计量已被安装并运行正常。智能计量设备运行一个计量应用，该应用以小时为单位将生成计量数据测量。智能计量设备运行一个配置有 <sclBase> 的 DSCL：<protocol>：//meter12345. utility 1. com/。

图 5-24 提供了一个 NSCL 和 DSCL 连同其相应的资源结构的图形化表示。

智能计量开始运行时，它会执行以下功能：

• 网络引导和网络注册：这些程序依赖于接入网络。网络引导包含配置具有所有必要参数的设备，以允许它连接并注册到一个网络。网络引导的例子包括来自普遍综合型电路卡（UICC，通常被称为 SIM 卡）的引导。一旦引导已完成，该设备将有必要的凭据进行身份验证，并为接入网络获得授权。

• 服务引导：这涉及永久 M2M 服务凭据的提供（身份、密钥等），这将用于与 M2M 服务层连接和注册。

5.7.4.2 NA 订阅注册智能计量

每当部署智能计量时，假设 NA 希望被告知。当在其 <sclBase> 的 scl 资源下注册 DSCL 时，这样做的一种可能的方式是订阅 NSCL 以便得到通知。在 ETSI M2M 架构中，通过一个特定的订阅资源的创建完成订阅。由于 NA 希望监察一个 <scl> 的创建，例如下面的 <protocol>：//smartmetering. utility 1. com/scls/，在

scl 订阅采集资源下需要创建订阅资源。图 5-25 为订阅提供了程序流程。

以下提供了消息流的细节：

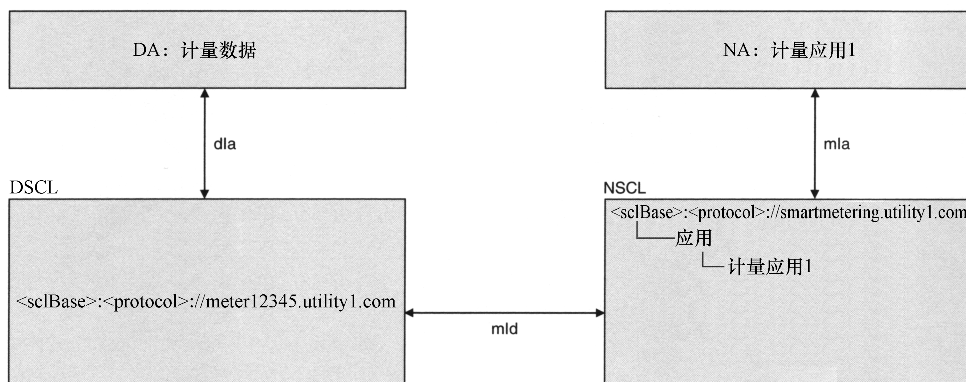


图 5-24　初始资源结构的图形化表示

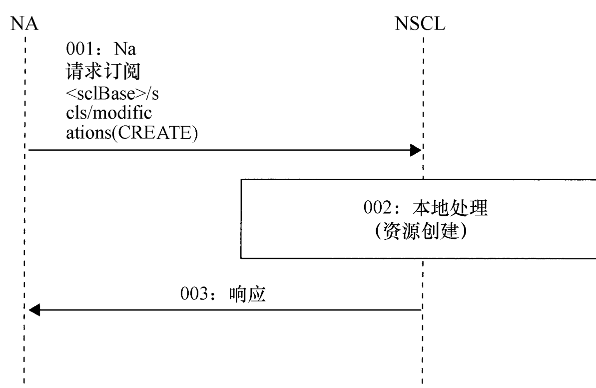


图 5-25　scl 资源的订阅

- 001：NA 在资源 < protocol > 下要求创建一个订阅实例：//smartmetering. utility1. com/scls/subscriptions/。NA 提供了实例的名称（在标准中不被要求）：newMeters。该请求也可以提供其他的参数，例如延迟传输，它提供了一个如何迅速地通知 NA 的指示。
- 002：NSCL 验证请求并且创建订阅。
- 003：NSCL 确认 NA 的资源创建。

直到智能计量注册到 NSCL 之前，通知将不会发生，这将被翻译成一个 DSCL 注册程序，如在下节中描述的。

5.7.4.3　NSCL 的智能计量注册

一旦已经执行引导，DSCL 可以执行 NSCL 发现和 SCL 注册程序。为了简单起

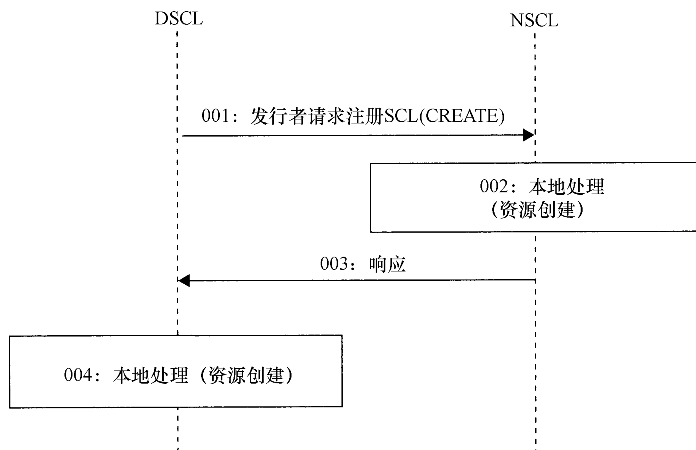


图 5-26　注册程序示例

见，此示例假设必要的信息，例如 FQDN[㊀]、端口号等，达到在智能计量设备上配置 NSCL 是必需的。这意味着 SCL 注册可以立即发生。图 5-26 为 SCL 注册提供了信息流。

执行下面的步骤：

- 001：在 <protocol>：//smartmetering. utility 1/scls/下通过一个资源的创建，DSCL 请求注册，采集资源标识符 12345，这是智能计量 SCL 的唯一标识符。
- 002：NSCL 确保 DSCL 有适当的验证以及 scl 资源名称，通常 DSCL 的一个配置标识符已经不存在于 <sclBase>/scls 采集中。然后以资源名 <protocol>：//smartmetering. utility 1. com/scls/meter12345 创建一个 scl 资源。默认属性，如期满时间被填充在资源中。
- 003：托管 SCL（这种情况中的 NSCL）积极响应请求。
- 004：DSCL 创建一个资源代表 NSCL，这并不需要为 DSCL 显示注册，因为只有 DSCL 和 GSCL 被要求为 NSCL 显示注册。

5.7.4.4　通知有关注册智能计量的网络应用

一旦 DSCL 注册了 NSCL，通过 NSCL 得到触发的一个自然程序将会通知与注册相关的 NA。图 5-27 提供了相应的信息流。

通知信息流的步骤如下：

- 001：在 scl 采集资源下创建一个 <scl>资源实例。这对应于一个智能计量的注册。

㊀ FQDN（完全合格域名/正式域名）是一个独特的域名名称，可以分解为一个使用 DNS 的网络地址。

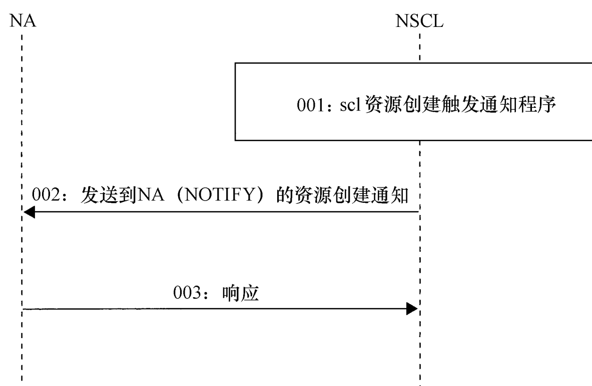


图 5-27　通知程序示例

- 002：NSCL 通知与一个新 SCL 注册相关的 NA，对应一个新智能计量的部署。
- 003：NA 承认收到通知。

5.7.4.5　DSCL 的设备应用注册

使用 dIa 接口，下一步将是对 DSCL 的 DA 进行本地注册。应用注册允许在本地 SCL 上创建应用资源（见图 5-28）。根据接入权限，在其本地 SCL 或远程 SCL 上允许一个应用操作资源也是一个必要的条件。因为 DSCL 已经注册了 NSCL，没有必要为 DA 注册 NSCL。

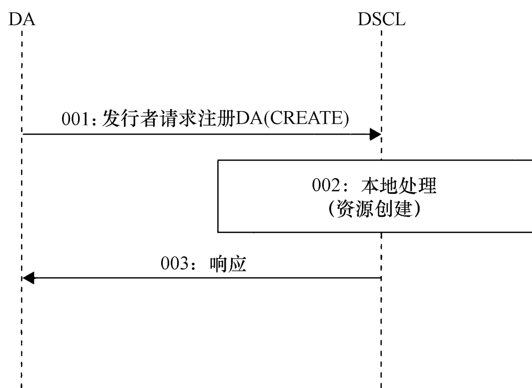


图 5-28　应用注册程序示例

- 001：对于应用采集实例，根据具有识别码计量数据的 <protocol>：//meter12345. utility 1. com/applications/，通过一个资源的创建，DA 要求注册，通过链接 <protocol>：//meter12345. utility 1. com/applications/meterData 可寻址。
- 002：DSCL 检查 DA 是否被授权，以创建注册资源。一旦这些检查已经完成，创建资源和 DSCL 更新相关的属性不由 DA 提供。DSCL 还可以为不由 DA 提供的任选属性提供默认值，这些都是从 SCL 策略推断出来的。例如：
  - DSCL 可能会由发行者降低被建议的到期时间。
  - 如果没有提供应用状态，托管 SCL 为“ONLINE”将设置应用状态属性。
- 003：DA 被告知成功的注册。

5.7.4.6　为 NSCL 公布一个注册的 DA

现在假设 DA 希望为 NSCL 公布其注册，以便 NA 可以发现所有的智能计量应用，该应用已成为可运营的。在这种情况下，DA 需要更新一个 DA 资源的特定属性 announceTo，以便为 NSCL 请求公布。相应信息流（见图 5-29）的细节如下：

- 001：DA 请求宣布其 DA 资源；通过原始更新的使用，设置一个 announceTo 属性特定值是可以做到的。
- 002：DSCL 确认请求的有效性，然后更新 DA 的 announceTo 属性。
- 003：为 DA 返回一个通用的响应，确认公布的请求对 DSCL 是可接受的。但是已经发生的实际公布没有确认。
- 004：DSCL 启动程序在 NSCL 上创建一个公布资源。
- 005：DSCL 请求在资源 <protocol>：//smartmetering. utility 1. com/scls/meter12345/applications/下创建一个新的子资源。该子资源将是 <application Annc> 格式，图 5-30 中显示了结构。
- 006：NSCL 验证接收到的请求，然后创建一个具有特定属性的公布资源。
- 007：NSCL 返回一个响应，指示创建是否成功。

图 5-31 提供了一个 NSCL 和 DSCL 的图形化表示，一旦 DA 已经为 DSCL 进行了本地注册，此图也为 NSCL 考虑了 DSCL 注册。

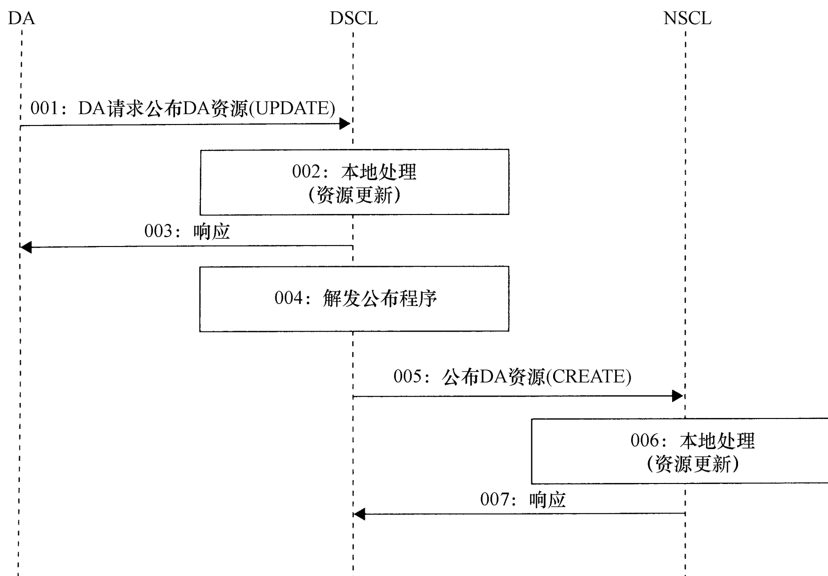


图 5-29　应用注册公布程序示例

5.7.4.7　通过使用存储器资源报告计量数据

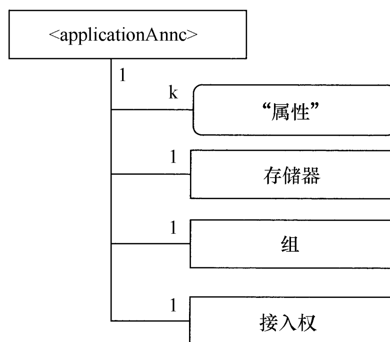


图 5-30　application Annc 资源结构

现在假设为了报告应用数据对 DA 编程。ETSI 102 690 规范允许多种选择做这项报告。通过使用存储器采集资源交换应用数据是可以做到的。正如图 5-22 所示，创建的存储器子资源有多个资源，例如，根据 < sclBase >、< scl >或 < application >。对于我们的特殊例子，合乎逻辑的选择是为了创建一个存储器采集资源，在 DSCL DA 应用资源 <protocol >：//meter12345. utility 1. com/applications/meterData/containers/meterDataSamples/或在 DSCL DA 公布资源 < protocol >：//smartmetering. utility1. com/scls/meter12345/applications/meterData/containers/meterDataSamples/。其中 meterDataSamples 是为了报告作为子资源的计量数据样本而创建的存储器采集。根据其业务需要和一些其他参数，如收费和网络使用，应用开发员需要作出最后的选择。对于我们例子的情况，在 NSCL 也就是公布的 DA 资源下，报告的实际计量样本会被公布。图 5-32 为最初创建的存储器采集提供了信息流。

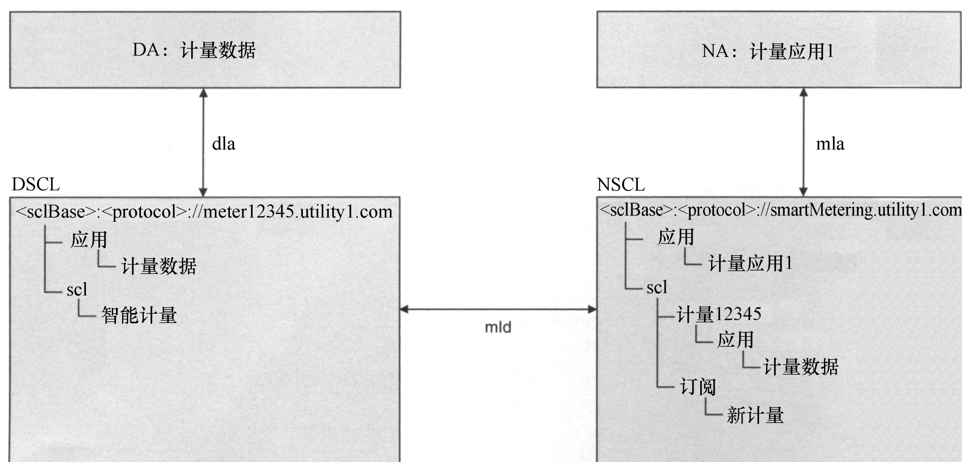


图 5-31　本地 DA 注册的以下公布的资源结构的图形表示

● 001：DA 在 NSCL 资源 < protocol >：//smartmetering. utility 1. com/scls/meter12345/applications/meterData/containers/下请求创建一个存储器资源。该请求的参数包含存储器采集的名称：meterDataSamples。

● 002：根据父资源的 URI，DSCL 认识到该请求涉及 NSCL 下的一个资源创建。

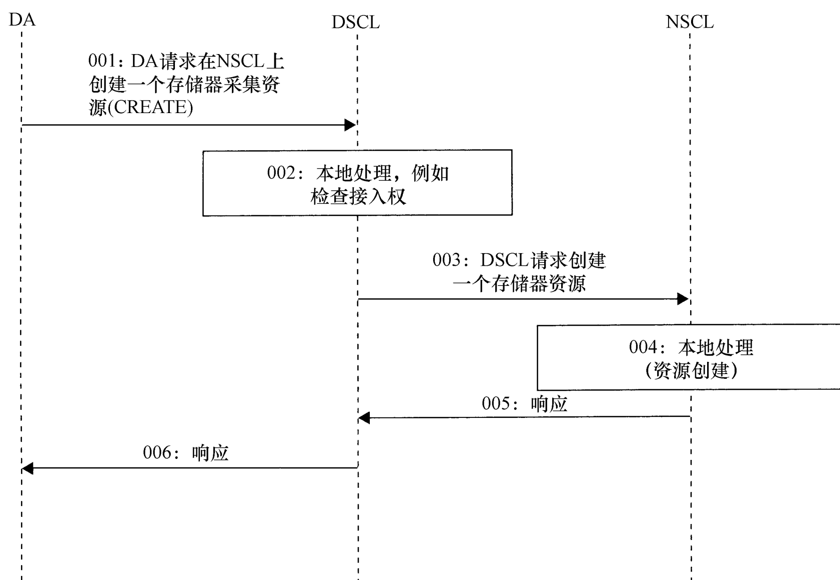


图 5-32 存储器资源创建程序示例

DSCL 执行必要的请求验证，任选的检查包括接入权限的验证。

- 003：该请求将被转发到 NSCL。
- 004：NSCL 检查请求的有效性，并且验证发行实体有必要的接入权限来创建资源。然后 NSCL 创建存储器资源和 DA 公布资源。最终的采集资源通过 <protocol>：//smartmetering. utility 1. com/scls/meter12345/applications/meterData/containers/meterDataSamples 进行寻址。
- 005：发回 DSCL 的一个响应。
- 006：在 005 中 DSCL 为 DA 转发应答，以确认资源创建。

用于创建存储器实例的程序将与刚才所描述的完全一样。因为存储器实例的创建根据采集将被完成，步骤 001 中的创建请求需要使用资源位置 <protocol>：//smartmetering. utility 1. com/scls/meter12345/applications/meterData/containers/meter-DataSamples/contentInstances。

5.8 本章小结

本章概述了基于资源的 ETSI M2M 架构。为 ETSI TC M2M 第 1 版提供了三个最重要功能的描述和资源结构，并且通过一个例子提供最重要程序的概述。

为了一个横向 M2M 服务平台，ETSI TC M2M 规范表示一个重要的步骤转发提

供基础水平。虽然最初的版本主要解决数据的调解、安全性和设备管理，可以预料未来版本在规范其他服务功能上要格外努力。

在编写时，ETSI M2M 规范仍在不断地变化，所以一些细节可能略有改变。本章的读者应该阅读有关的系统/架构方法，考虑有关详细信息，请参考规范的最终版本。本章集中在第二阶段方面（架构和信息流），并且故意不处理协议例子。同类书《物联网，关键应用和协议》中提供了一些协议例子。

参考文献

[3GPP TS 23.060] 3GPP TS 23.060. General Packet Radio Service (GPRS). Service description. Stage 2 (2011).
[3GPP TS 23.401] 3GPP TS 23.401. General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access (2011).
[BBF TR069] Broadband Forum TR-069. Amendment 3 CPE WAN Management Protocol (2010).
[ETSI TS 102 690] ETSI TS 102 690: Machine-to-Machine communications (M2M); Functional architecture; v1.1.1, 25 Oct 2011.
[G.hn] ITU-T Recommendation G.9960. Next generation Home Networking Transceivers Foundation (Copper-pair, Powerline and coax PHY Layer) (2010).
[OMA DM] OMA-AD-DM-V1_3. Device Management Architecture, Version 1.3 (2010).
[Yankee Group] Yankee Group (2010) A Closer Look at M2M Carrier Strategy, Market Research Report.

第 6 章　公共移动网络中的 M2M 优化

Toon Norp[1]，Bruno Landais[2]
[1]荷兰应用科学研究组织，代尔夫特，荷兰
[2]阿尔卡特朗讯公司，Lannion，法国

6.1　概述

许多 M2M 应用使用公共通信网络从 M2M 设备到 M2M 服务器传输数据。这些通信网络将必须进行调整，以配合 M2M 应用的预计增长所产生的通信。随着越来越多的 M2M 应用得到介绍，在不久的将来，越来越多的设备将被连接到现有的网络。这些 M2M 设备相比于以人为本的设备在通信网络上将有一个非常不同的效果。本章介绍了公共通信基础设施上 M2M 具有的影响，并且描述了一些方法，网络运营商将用 M2M 通信，以优化他们的网络。

通信网络为 M2M 应用将提供数据通信和相关的增值服务。需要注意的是，具有 M2M 服务等级的产品，通信运营商寻求提供更多简单的 M2M 数据通信。一些运营商在 M2M 的基础上甚至提供了完整的归属安全服务。然而，在本章中我们将限制自己的 M2M 通信的数据通信部分。

本章的重点是移动网络中的 M2M。对于 M2M 应用所有者，对于控制订阅和数据连接的端到端的可见性，移动网络往往是更合适的。从操作者的角度来看，移动网络要应付更多的挑战，为了迎合大量的 M2M 通信，优化是必要的。不过，许多事项、问题和讨论的解决方案是通用的，也将适用于固定网络。

为了迎合 M2M，本章的目的是显示通信网络所需要的网络改善。尽管如此，本章为 M2M 应用所有者、M2M 应用提供者和移动行业以外的其他人提供一个 M2M 网络事项的更好理解。

在 6.2 节中，在公共通信网络的基础上给出了 M2M 的一个概述。6.3 节中，重点是公共通信网络的优化，使其更好地适用于 M2M。

6.2　基于通信网络的 M2M

6.2.1　引言

许多应用为其数据传输使用专门的基础设施。例如，为了监测温室中盆栽植物

的水位，一个私有的本地无线基础设施可能是最简单的解决方案。然而，有许多 M2M 应用，其中的公共通信网络使用是比较合适的。例如，一个电子健康应用中的门诊患者在家是被远程监控的，这将不得不依赖公开地可用的通信网络。

本章中，我们考虑 M2M 应用如何使用公共通信网络和这些网络上的 M2M 应用的请求。公共通信网络上的 M2M 应用的影响与传统的通信服务的影响是完全不同的。M2M 通信主要包括数据通信。然而，即使 M2M 数据传输与当今（移动）宽带互联网服务进行比较，我们仍能看到许多差异。对于通信运营商，考虑他们如何必须为 M2M 通信准备他们的网络是很重要的。假设 M2M 通信在相当一段时间里将继续发展，可能到一定的水平，它将超过通信的传统类型。如果公共通信网络只对人对人通信和互联网接入进行优化，然后连接大量的 M2M 应用，该应用在这些网络的效率和对它们提供的服务上产生负面的影响。

对于 M2M 应用所有者和 M2M 应用开发商，通过运行其自身的应用了解基本公共通信网络是有兴趣的。在 M2M 应用如何组织它们的数据通信中，一个细微的差异可以形成一个巨大的影响差异，这些应用存在于公共通信网络中。对于 M2M 应用所有者底层网络将是有效的，设计 M2M 应用是友好的，作为运营商很可能考虑 M2M 应用的影响，该应用存在于具有其定价结构的网络中。

下面的 6.2.2 节将首先介绍 M2M 通信方案和在这些网络中公共通信网络所发挥的作用。6.2.3 节将对于 M2M 通信讨论是使用固定还是移动通信网络。最后，6.2.4 节将解释 M2M 应用的要求种类，该应用通过一个公共通信网络存在于数据连接上。

6.2.2　M2M 通信方案

在大多数 M2M 通信方案中，许多 M2M 设备与一个中央服务器进行通信。这样一个设备到服务器通信方案的例子将是一个远程采集其所有客户计量读数的能源集团。设备数量的范围可以从使用 M2M 车队管理应用的小货运公司的几十个到大型能源企业的数百万个。

如图 6-1 所示，设备到服务器通信方案中设备到服务器确实没有一个 N:1 的比例。可能有多个服务器，例如，用于负载平衡或冗余。然而，M2M 设备的数量通常比 M2M 服务器的数量要大得多。此外，大多数 M2M 设备不必关注它们与哪一个特定的 M2M 服务器进行通信。M2M 设备仅仅为与一个服务器通信进行了配置，并且不必作出服务器选择的任何形式。

在一个真正的设备到服务器方案中，公共网络运营商提供了 M2M 设备和 M2M 服务器之间的连接。通常情况下，网络运营商不为 M2M 设备的个人所有者提供此连接，而对 M2M 应用所有者提供此连接。在一个设备到服务器方案的基本例子中，M2M 应用所有者拥有所有的 M2M 设备和 M2M 服务器。另外，M2M 应用所有者实际上不可能拥有 M2M 设备，但拥有数据通信订阅。例如，一个车辆导航设备

的制造商可能出售导航设备，该设备具有实时交通信息和兴趣点的订阅。虽然导航设备销售给终端顾客，但是导航设备的制造商拥有移动数据订阅，该订阅需要为导航设备传输消息。

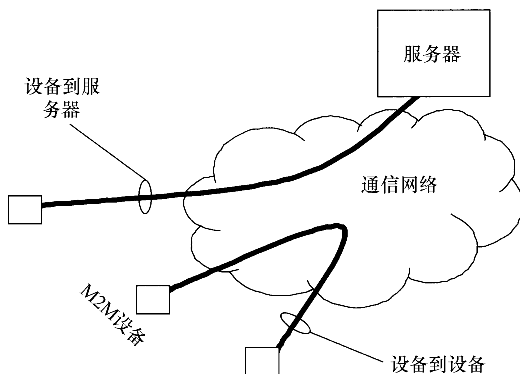


图 6-1 设备到服务器和设备到设备的通信方案

需要注意的是，网络运营商在 M2M 设备和 M2M 服务器之间可以提供更多的通信。他们也可提供基于实际 M2M 服务器的服务能力。然而，对于本章的目的，我们专注于公共网络运营商在其数据通信提供者中的角色。在这个意义上，网络运营商可以被视为对其自身内部 M2M 服务提供者提供数据通信服务。

尤其是当网络运营商提供具有基于网络接入的 M2M 服务功能时，端到端的通信路径（见图 6-2）也将涉及 M2M 用户。例如，该 M2M 用户将会接入 M2M 服务器采集的计量数据。M2M 用户和 M2M 服务器之间的通信没有具体的 M2M 特征。通常，使用一个基于互联网的界面可以运行在通信网络的任何类型上。

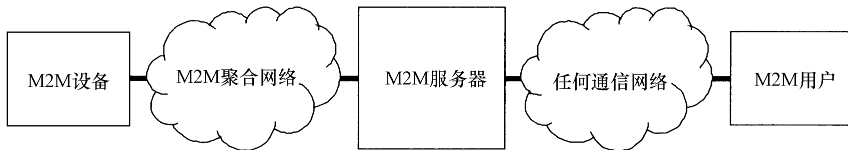


图 6-2 通过 M2M 服务器的 M2M 通信路径

如图 6-1 所示，也有一个通信方案中 M2M 设备与没有 M2M 服务器参与的设备相互直接进行通信。这样一个方案的例子是一个应用，在客户的房子中，一个摄像头与一个媒体服务器远程同步。另外一个例子可能是一个房屋报警系统，例如它通过给他或她的电话发送一个信息直接与业主进行连接。需要注意的是，直接的设备到设备通信与通过一个 M2M 服务器在两个 M2M 设备之间进行通信是不同的。例如，在一个多用户游戏中，两个游戏会话涉及相同的游戏会话，不仅可以与相同的

游戏服务器相连，还可以与相互没有涉及服务器的会话直接相连。设备到设备的通信方案仍远不及构成大量 M2M 通信的设备到服务器的方案普遍。然而，未来越来越多的不同种类设备成为连接的，直接的设备到设备通信的可能性将会增加。

随着设备到设备的通信，M2M 设备需要能够选择它们希望与其通信的其他 M2M 设备。因此，有一个 *M*:*N* 的连接。该业务方案在所有可能性中有所不同。一个单一的 M2M 应用所有者拥有所有涉及通信的 M2M 设备是没有必要的。在这个意义上说，设备到设备的通信方案非常类似于我们熟知的通过服务器例如电话的通信方案。

当单个领域中有大量的 M2M 设备时，采取 M2M 网关（GW）方案（见图 6-3）可能是有利的。在 M2M GW 方案中，许多 M2M 设备通过公共通信网络可以分享单个连接。对于 M2M 设备和 M2M GW 之间的通信，使用一个本地网络技术（如 LAN、WLAN 或 ZigBee）。

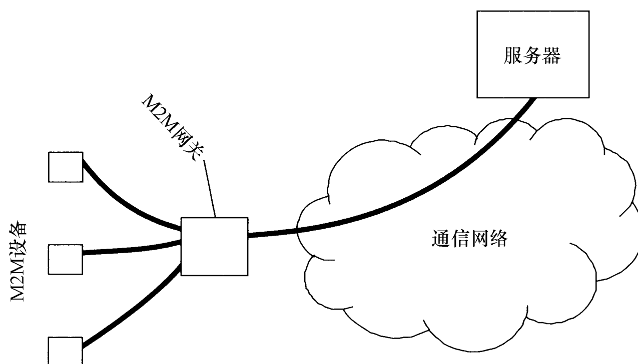


图 6-3　M2M 网关方案

6.2.3　移动或固定网络

从广义上讲，公共通信网络是固定的或者是移动的通信网络。网络的类型可以被用于 M2M 应用。然而，如今的 M2M 重点是移动通信网络。

对于许多 M2M 应用，移动通信显然是唯一的选项。货运公司的一个跟踪和追踪应用显然不以一个固定的通信解决方案工作。然而，对于这些情况，其中的 M2M 设备不是移动的，移动通信往往是首选。特别是对于不同未知的 M2M 设备，连接到一个固定的网络可能是昂贵的。进行水管理的例子是灌溉水泵、水闸门和其他设备。这种设备通常位于一个乡村环境，远离任何其他建筑物或基础设施。因此电缆连接到这些位置是非常昂贵的。

此外，在这种情况下，M2M 设备安装在私人住宅或办公室中，移动通信往往是首选的解决方案。这是因为 M2M 应用所有者与固定的网络订阅的业主往往是不同的。在这种情况下，M2M 应用所有者不希望依赖于固定网络订阅的所有者。

在图 6-4 中，我们考虑一家希望直接连接到电表的能源公司的例子。在这种情况下，能源公司是 M2M 应用所有者。能源公司的大多数客户（A 到 D）将有固定网络连接的某种形式，这种连接用于连接能源电表。然而，一些客户使用固定的网络运营商 A，其他的是固定网络运营商 B 的客户。如果能源公司想利用现有的固定网络连接，固定网络运营商的客户选择将必须适应其技术解决方案。在以下情况中，客户没有一个固定的网络连接，或者一个电力网关中断并且禁用固定网络归属网关，进一步复杂一个基于固定网络的解决方案。另外，能源公司处理一个手机用户 A，以获得手机订阅，并且在所有的电表中插入一个 SIM 卡。

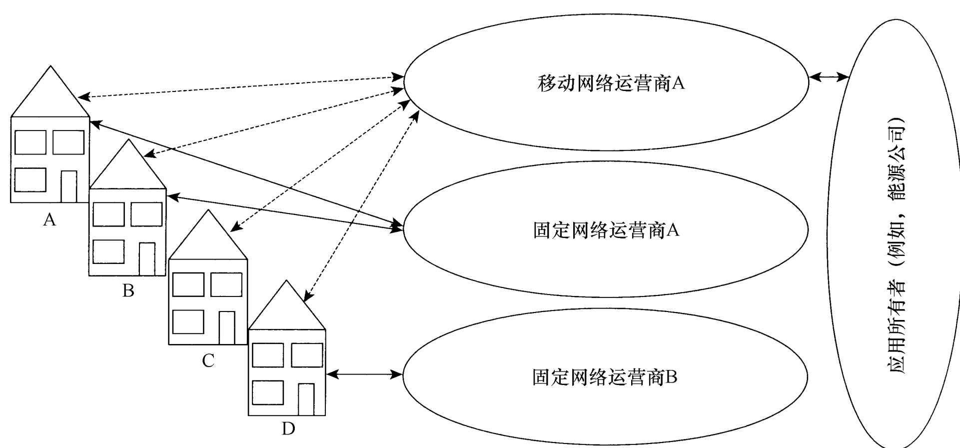


图 6-4 通过移动网络 M2M 创建运营商的独立性

为 M2M 设备使用移动网络，该设备不是移动的，也有其劣势。M2M 设备可以位于移动网络的覆盖不是特别好的区域的室内。当为移动 M2M 设备使用移动网络时，一个位置的不好的移动覆盖甚至将超过其他位置的好的覆盖。然而，位于一个不好的覆盖点的一个静止的 M2M 设备将永远无法发送数据。

覆盖范围问题的一个解决方案是使用一个漫游的 SIM 卡。当使用来自一个特定国家运营商的 SIM 卡时，它通常只适用于其归属网络运营商，因为一个国家的运营商之间的国际漫游不是常被支持的。因此在该事件中，归属网络运营商不提供一个特定位置的足够覆盖，没有后备解决方案。然而，如果一个外国移动网络运营商的 SIM 卡被使用，M2M 设备将首先尝试首选的网络运营商，但是假设归属网络运营商有相关的漫游协议，它也可以使用所有其他可用的移动通信网络。使用漫游 SIM 卡的一个缺点是漫游费将导致数据通信的成本较高。然而，对于 M2M 应用发送非常少的数据，这是一个小问题。因后勤原因，漫游 SIM 卡也被使用；例如，对于每个销售相框的国家，数码相框制造商可能希望避免使用一个专用 SIM 卡的后勤问题。普遍预计占 M2M 设备非常大的百分比的将是半永久性的漫游。

6.2.4　M2M 应用的数据连接

不同的 M2M 应用有非常不同的通信需求。很明显，一个携带 24/7 视频数据的监控摄像机应用在数据通信上相比于只需要发送少量数据的自动售货机应用处于一个较高的要求，例如，一个特定的产品是脱销的。即使有类似的 M2M 应用，单个应用的要求仍然是非常不同的。希望引入智能计量应用的两个能源公司在特定的参数上可以有非常不同的要求，例如如何经常记录电表数据。

列出特定的 M2M 应用的特性是不可能的，因为有太多简单不同的具有不同特点的 M2M 应用。但是，区分被用来表征不同 M2M 应用的特定方面是可能的，例如：

- 数据容量- M2M 应用发送多少数据？
- QoS 需求- 对其数据传输 M2M 应用有什么 QoS 需求的种类？
- 时间敏感性- 应用需要直接的数据通信或者应用可以延迟数据通信几小时吗？
- 通信方向- 具有一定的 M2M 应用，M2M 设备总是启动数据通信，其他的 M2M 应用需要 M2M 服务器，以便可以启动数据通信。

表 6-1 给出了一些具有其通信需要的 M2M 应用的例子。需要注意的是这些仅仅是示例，因为有更多的 M2M 应用和类似的 M2M 应用可能有非常不同的特点。

表 6-1　不同的 M2M 应用有不同的通信需要（由 TNO 的许可复制）

		数据量	服务器的质量要求	时间敏感性	通信指导
	监控摄像机	高	高	高	初始的网络
	能源电表	低	低	低	初始的网络
	快速管理	低	低	中等	初始的设备和网络
	电子书阅读器	高	低	中等	初始的设备
	媒体同步	高	低	中等	初始的设备和网络
	销售终端点	低	中等	高	初始的设备

M2M 应用的通信方向要求对多数网络中的通信设置是很重要的。网络是面向连接的，连接首先需要在数据通信进行之前得到设置。许多网络，如 GSM/UMTS 分组交换网络，不支持启动的网络连接安装㊀。在无连接网络中就不需要建立连接。但是在无连接网络中，防火墙和网络地址转换可以是初始的网络通信的一个瓶颈。通常，在防火墙和网络地址转换中的针孔和转换是由初始的设备通信来配置的。当寻址 M2M 应用需要发起的网络通信时，这将成为一个问题。

为了在服务器的请求上建立一个发起的设备连接，需要使用“触发”。在触发下，M2M 服务器可以为设备发送一个指示，该设备可以与 M2M 服务器建立通信。在目前的移动网络的 M2M 应用中，使用触发是由于少数请求网络的分组数据协议（PDP）建立环境程序。M2M 服务器发送一个触发到 M2M 设备，以一个 SMS 或交换电路（CS）的电话呼叫建立的形式。收到一个特殊格式的 SMS 之后，设备为 M2M 服务器设置一个数据连接（即 PDP 环境）。此外，在一个 CS 呼叫设置的情况下，设备不接听电话但是为 M2M 服务器设置一个数据连接。一般来说，设备已经配置了 M2M 服务器的地址，所以需要触发指示。

在面向连接的网络中，考虑何时建立和拆除数据连接是重要的。一个数据连接建立的相关信令相比于许多 M2M 应用发送的数据可能是一个显著的开销。对于一个频繁发送数据的设备，连续的数据传输之间保持数据连接处于活跃状态是更有效的。连接建立和拆除的相关信令相比于保持连接打开将会消耗更多的资源。但对于很少发送数据的应用而言，拆除数据脉冲串中的数据连接是更有效的。

对于移动网络中的 M2M，考虑是否当它们不发送数据时要保持设备连接，这也是很重要的。在许多网络中，在进行可能的通信之前，该设备还必须注册并提供网络的身份验证。在 GSM/UMTS 网络中，注册采取一种连接程序的形式。当一个设备连接到网络时，移动性管理将被执行。这意味着网络跟踪设备的位置，以及位置区域的粒度。通过寻呼已知位置区域的设备，网络可以为设备建立一个连接。对于 M2M 应用需要能够启动数据通信，网络需要知道在哪里进行寻呼设备。保持连接的设备确保网络有这一消息。另一方面，对很少发送数据的设备，移动管理信令相比于大量发送的用户数据将是一个重要的开销。如果还有不需要触发的设备，那么当其不通信时分离设备是更有效的。

如果我们注重不同的应用有怎样不同的活动模式，以上描述的连接的基础是很重要的。活动模式非常确定数据通信的效率。

图 6-5 示出了一个 M2M 设备活动模式的一个典型例子。它可以代表执行一个状态更新的自动售货机。首先，在创建数据连接之前，设备连接到网络。少量的数

㊀ 3GPP 标准定义了一种网络需求的 PDP 环境下的激活程序，但很少使用该标准。

据传输之后，没有更多的数据发送并且连接被释放。连接释放之后，可能遵循一个分离程序（没有显示）。不同 M2M 应用的数据连接建立的优化取决于它们的数据通信模式。发送少量数据的设备要求优化，不同于频繁发送数据的设备。图 6-6 显示了一些数据通信模式的示例。数据通信模式的特点可以区分不同 M2M 应用之间的差异。有些应用不断地发送数据，而另一些在发送一个数据脉冲串之前可能需要超过 15 年的等待。

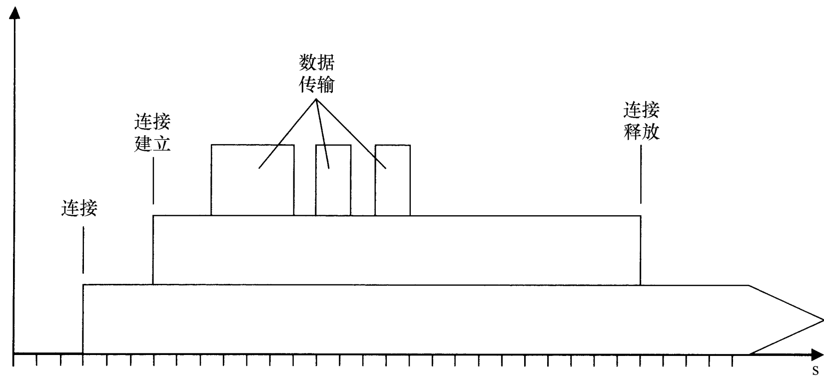


图 6-5　蜂窝移动网络中的数据连接确立

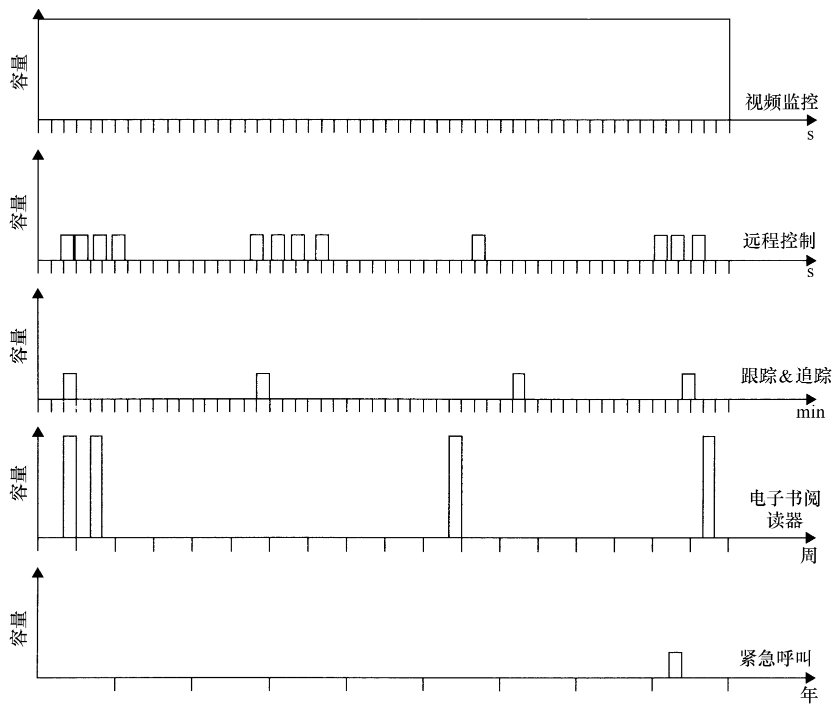


图 6-6　具有不同通信模式的不同 M2M 应用

图6-6 中的视频监控应用将不断地产生数据。在这种情况下，连接、创建和维护一个连接是更有效的。此外，对于远程监控，保持持续的连接是最好的。在这种情况下，数据发送到脉冲串中需要几秒钟的时间间隔。拆除数据脉冲串之间的连接是可能的，但是创建和拆除连接比保持连接打开消耗更多的资源。在一个跟踪和追踪应用中，数据脉冲串之间的时间间隔变得很长（例如，每 15min 一次）。现在是最好保持两个数据的脉冲串之间的连接开放还是释放连接开始值得商榷。对于电子图书阅读器应用，数据脉冲串之间的时间间隔变得更长。在网上购买书籍可以间隔有几周。当不买书时没有必要进行连接。在一个紧急呼叫应用中，当汽车涉及一个应急响应时，它会自动连接急救中心。在这种情况下，紧急呼叫应用发送任何数据之前将有望花费好多年时间。这些年一直保持 M2M 设备连接是一种浪费，特别是保持连接打开。

6.3 M2M 的网络优化

6.3.1 引言

如今公共通信网络不再是为 M2M 应用而设计的。这些网络原本是为电话通信设计的。即使分组交换通信和下一代网络出现以后，M2M 通信的网络仍然没有得到优化。如今分组交换通信网络最大的优化是给终端用户提供宽带互联网接入。然而，为大量的 M2M 设备提供 M2M 数据通信，并且为 M2M 应用所有者而不是终端用户提供服务意味着一种不同的网络优化。当今的分组交换通信网络的架构将不再需要一个全面的改革，而是一些显著的变化，这些需要的变化将支持一个真正不辜负其承诺的 M2M 市场。

M2M 网络优化分为五个不同的类别：

- 降低成本-为提供 M2M 数据通信降低了网络运营商的成本。
- 增值服务-可以使网络运营商提供 M2M 特定的增值服务。
- 触发优化-为初始网络的 M2M 运营程序提供改进的支持。
- 过载和拥塞控制-确保 M2M 应用的高负荷不会造成网络中断。
- 命名和寻址-保证在一个数十亿 M2M 设备得到连接的时期中仍然会有足够的标识符和地址。

下节首先介绍了 3GPP 与移动网络的网络优化标准的相关活动。该节的其余部分阐述了 M2M 网络优化的不同类别。

6.3.2 3GPP 机器类通信网络改进的标准化

有几个标准化开发组织致力于 M2M 标准化。然而，移动网络的标准化组织 3GPP（第三代合作伙伴计划，www.3gpp.org）显然在规范 M2M 网络优化上是最先进的。

在 3GPP 中，2008 年服务和需求组织 3GPP WG SA1 在机器类通信的网络改进上成立了一个工作项目。这项工作的目的是定义 M2M 的服务需求。3GPP 指的是作为机器类通信的 M2M，也指的是考虑机器与人类进行通信的可能性（M2H 或 H2M 通信）。

3GPP WG SA1 中的这项工作已经导致了一个需求规范的文档 3GPP TS 22.368 “机械器类通信（MTC）的服务需求；阶段 1” [22.368]。在共同服务需求之间的这个规范中作出了一个区分，该需求适用于所有的 MTC 设备、订阅和 MTC 功能，这将只适用于特定的订阅。MTC 功能背后的思想是在每一个订阅基础上运营商可以区分他们特定的 M2M 应用的产品。根据 3GPP 版本 10，[22.368] 的第一版已完成。

[22.368] 中的 MTC 服务需求是基于其他 3GPP 组织中的架构和协议规范。然而，很明显 [22.368] 比 3GPP 组织中的架构和协议规范包含更多的需求，3GPP 可以在一个单一的释放中处理。在版本 10 中，仅过载和拥塞控制相关的功能已完全指定。即使是版本 11，体系结构和协议规范工作只集中在 [22.368] 中定义的一小部分功能。表 6-2 给出了版本 10 和版本 11 功能的指示性清单。

表 6-2　3GPP 版本 10 和版本 11 中机械类通信特征的网络优化

3GPP 版本 10	扩展接入限制
	无线资源控制中的低接入优先级指示
	无线资源控制中的扩展等待时间
	下行链路数据通知请求的节流
	基于 APN 的拥塞控制
	一般核心网络移动性管理控制
	防止 PLMN 重选的过载优化
3GPP 版本 11	触发优化和触发架构
	寻址优化和依附于电话号码的移动

在不同的体系结构和协议规格中指定 [23.888] 之前，MTC 网络改进的主要问题和架构解决方案是第一个在具体的 MTC 技术报告 3GPP TR 23.888 “机器类通信（MTC）的系统改善”中被研究的对象。在一些指定的规格中可以找到 MTC 的 3GPP 规范的体系结构规范（例如，[23.682] 中指定的与外部 M2M 服务器的相互作用，[23.060] 和 [23.401] 中指定了分组交换（PS）核心网络的 MTC 详情，在 [22.011] 中一起指定了扩展接入限制（EAB）和其他接入控制机制）。

工作在 MTC 网络改进上的 3GPP 可能会持续相当长的一段时间。在 [22.368] 中有各种各样的需求将必须在版本 11 以后的版本中得到实施。此外，3GPP WG SA1 还定义了新的需求。在 [22.888] 中，新的需求例如设备到设备通信和网关方案正在研究。

6.3.3　降低成本

许多 M2M 应用必须是低成本的。例如，智能电表数据通信的成本相对于每家

每户的电费成本应该没有显著的增加。这同时也意味着网络运营商的收入较低。与一个宽带互联网接入订阅的平均收入相比，平均的 M2M 订阅产生的收入将明显减少。为了使 M2M 通信服务的供应经济可行，提供 M2M 数据通信成本将必须降低到一个最低限度。

对于运营商，降低每比特数据通信的成本始终是有吸引力的。但是随着 M2M 数据通信，利用 M2M 应用的具体性质进一步降低成本是可能的。例如，网络运营商可以和 M2M 应用所有者进行谈判，M2M 应用的数据通信仅限于网络的繁忙时期以外。对于网络运营商，这意味着没有必要向网络容量提供额外的投资。对于 M2M 应用所有者（取决于 M2M 应用），完全可以接受在非高峰时期被限制每天发送的数据。

对于网络运营商，将 M2M 数据通信与其他的数据通信区分开是很重要的，例如宽带互联网接入。如果 M2M 数据通信的特定限制可以导致更低的成本，那么网络运营商可以以一个较低的 M2M 应用价格进行谈判，该应用可以支持这些限制。然而，降低所有数据通信的价格以达到一个可以接受的平均价格水平，M2M 应用所有者可能从其他那些可以接受高价的数据通信用户那里获取收入。我们的目标是将 M2M 投资组合与为了吸引许多不同的 M2M 应用而由限制以及增值服务组成的一个正确组合区分开来。

为了寻找 M2M 应用中降低成本的机会，首先调查成本动因和网络成本组成部分是很有用的。表 6-2 所示为移动通信网络中的 M2M 成本动因。定义最重要的成本动因取决于 M2M 应用的类型。车辆远程诊断的 M2M 应用中，同时可连接的设备数目将是一个重要的成本动因：每一辆汽车可能每年只被监测几次，但是为了可获得，汽车中的 M2M 设备需要一直被连接。另一方面，对于公共交通巴士的一个监视摄像机应用程序，同时连接的设备的数量不再是一个重要的问题。连续视频画面传输的数据量将是一个更大的成本动因（见表 6-3）。

表 6-3 移动通信网络中一个 M2M 应用的成本动因（由 TNO 许可复制）

成本动因	网络成本组件	示例应用
基于组的订阅数目	SIM 卡；E.164 编号；HLR 能力	很少发送数据，并且仅由初始设备的应用（如报警）
同时连接的设备数目	网络节点中的移动性环境数据；移动性管理信令	很少发送数据，但是必须是可获得的应用（例如远程管理）
同时保持数据连接的数目	网络节点中的会话环境数据；防火墙能力；IP 寻址	需要连续地发送和接收数据（例如远程控制）的应用
数据会话的数目	连接建立信令；RADIUS/Diameter 能力；CDR 处理	定期地建立一个发送少量数据的连接的应用（如计量）
数据吞吐量	无线能力；传输网络能力；网络节点能力	高带宽应用，例如视频监测

许多 M2M 应用所有者有大量的订阅。对于具有智能计量应用的一个能源公司而言，订阅的数量将扩大到数百万。大多数这些订阅基本上是相同的。例如，QoS 配置的服务配置选项与订阅没有差异。因此通过不转载每个订阅的服务配置数据来节省用户数据库存储是可能的，但是所有的订阅指的是一个共同的服务配置。这将创建一个基于组的订阅。

对于 M2M 应用所有者，基于组的订阅也可以更容易地管理。如果应用需要更改服务配置文件，这个更改可能需要适用于所有的个人订阅。为每个个人的订阅逐个执行此更新体现了一个携带错误和不一致数据风险的巨大任务。通过改变常见的服务配置文件，携带所有订阅的服务配置文件更改是更容易的。基于组订阅的一个缺点是，为了指出哪个订阅属于哪一组需要一个管理过程。

基于组的订阅也将影响注册手续。通常在一个注册过程中，将服务配置数据从用户数据库下载到服务控制节点（例如，SGSN、MME 或 S-CSCF）。当数据库中的订阅数据有变化时，服务控制节点中为了改变数据需要一个更新程序。如果 M2M 通信的此更新程序没有得到改善，公共服务配置中的一个更改将有可能导致数百万计的个人服务配置数据更新，这些更新将同时被推到服务控制节点。这将在网络上产生一个危险的负载。一种可能的解决方案也是参考服务控制节点中的一个公共服务配置文件。每当至少有一个来自注册到服务控制节点上的订阅组的订阅时，公共服务配置数据将被下载。现在公共服务配置数据的一个更新只需要服务控制节点中下载的公共服务配置数据的更新。

通过结合组中所有订阅的收费数据，基于组的订阅也可以帮助降低相关的收费成本。没有基于组的订阅优化，每一个单独的订阅产生收费数据记录（CDR）。这意味着对于具有百万有效设备的 M2M 应用将生成百万 CDR。处理所有的这些个人 CDR 是昂贵的。CDR 需要被生成、收集、调解、存储，并形成一个账单。需要注意的是，据报告一个单一的 CDR 中的数据量实际上可能比 M2M 应用用户的数据量要大。运营商和 M2M 应用所有者是否必须同意基于组的收费应用。网络运营商可能会为同意基于组收费的 M2M 应用所有者提供一个较低的价格。基于组收费的一个缺点是，M2M 应用所有者不能区分（不常见的）单个设备的使用模式，因为这样的使用模式可以被用于例如识别欺诈情形。

当组中的许多订阅使用生成 CDR 的相同的网络节点时，基于组的收费数据效果最好。这将意味着，对于生成 CDR 的每个服务节点，始终只有一个组的单一的 CDR。当基于组收费应用时，服务配置数据中的订阅收费特性的一个新选项将需要被添加为指示。是否应用基于组的收费，需要通知生成 CDR 的网络节点。以同样的方式这是可以做到的，其中其他的订阅收费特性（例如，邮资后付/预付）均有分布。

另一个基于组的优化是基于组的监督。网络运营商一般适用于公平使用的策略，例如，数据传输的最大体积被设置为一个特定的订阅。一个网关节点计量订阅的传输数据，如果超过这个限额就采取措施。对于个别不发送大量数据的 M2M 应用，这些基于订阅的公平使用的策略不会产生很大的意义。但是由于大量的 M2M 设备可能会产生大量的数据，所以基于组的公平使用策略可能会更有意义。

在基于组的监督下，网关节点全体估量一个组中所有设备的使用数据。在一个中央在线计费服务（OCS）平台上，通过所有的网关节点监视一个组中所有设备的总用量。当每天、每周或每月达到极限已经得到判定时，采取措施，如减少该应用的吞吐量。例如，通过降低每个设备的单个数据连接的最大吞吐量，这是可以做到的。监督网关节点上的吞吐量将变得更容易，当突破一个特定的吞吐量时丢弃报文。这种方法的问题是，不知何故必须“共享”设备的一个吞吐量，该设备可以通过不同的网关节点连接；不保证一个单一的网关节点将被用于所有属于同一组的设备。

第三个基于组的优化是基于组的触发。当一个 M2M 应用所有者希望触发 M2M 设备的一个特定批次时，基于组的触发可以同时被广播到所有设备。假设 M2M 应用所有者有一定的需要被触发的 M2M 设备位置的知识水平。除了 M2M 应用最大化，其他所有网络范围内广播将效率不高。当发生大批的 M2M 设备同时被触发时，也应该采取保护。如果所有这些设备通过连接到 M2M 服务器同时反应，这可能会导致网络过载。

M2M 设备可能属于不同的组。例如，M2M 应用所有者可以使用一个组集来指示一个特定型号或版本的设备，而其他组集可以被用来指示运营商收费安排的一个特定格式。然后任何特定的订阅就可以属于多个组。然而，允许订阅属于多个组显著地复杂了订阅管理、服务和配置的相关程序。因此 3GPP TS 22. 368 中的 3GPP 已经指定任何订阅必须始终只属于一个组。这个限制的实际影响是有限的：M2M 应用所有者希望区分五种不同的设备型号和两种不同的收费管理，这两种收费管理可以简单地定义 10 个不同的组。

为了确定订阅程序和相关的服务配置程序中的特定组可以定义一个组标识符。在这种情况下漫游需要得到支持，组标识符必须是全球唯一的。通过在组标识符前面包含一个运营商标识符这是可以做到的。图 6-7 所示为一个组标识符如何被用在一个基于组订阅的数据模型中。

6. 3. 3. 1 设备不进行发送时降低其网络资源

M2M 设备甚至在它们不发送数据时仍然占用网络资源。一个例子是包含在连接网络或移动网络案例中的会话环境数据，连接设备的移动性管理环境。分组交换移动核心网络配备的大小参数广泛使用同时数据连接和同时连接用户。这意味着网络运营商将在保持连接或附属的 M2M 设备的网络配备中投资更多。此外，防火墙

功能和所需的 IP 寻址范围取决于同时连接的数量。

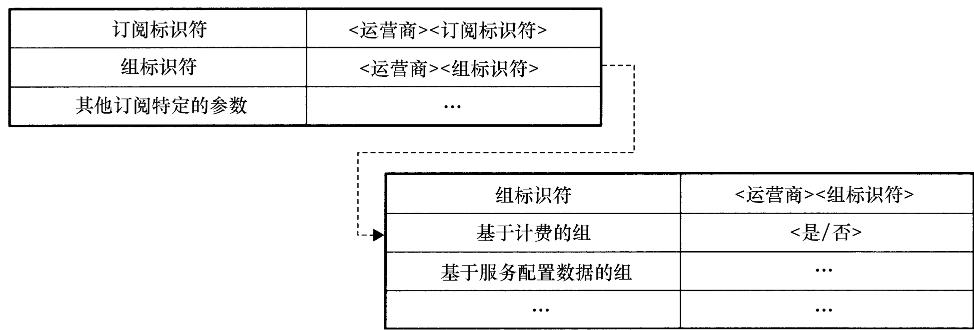


图 6-7　基于组订阅的示例数据模型

根据 M2M 应用的通信模式（见 6.2.4 节），当 M2M 设备不存在需要发送的数据时，断开或分离 M2M 设备可能是更高效的。通过删除环境数据并且所需的信令连接和重新连接数据发送的下一时刻，节省的网络资源之间有一个权衡。理想的平衡取决于所使用的网络技术㊀，附属和/或连接并且与保持环境数据相关的成本是很容易的。没有明确的规则，但是每隔 3min 发送数据的一个应用可能对保持连接是最好的，而每天只发送一次数据的一个应用可能对保持分离是最好的。

当设备不发送数据时降低其网络资源是只适用于网络运营商的一种成本优化。M2M 应用所有者可能会喜欢保持设备的连接和附属。例如，分离 M2M 设备意味着它们是不可到达 M2M 服务器的。保持 M2M 设备断开连接意味着它们必须得到触发以建立连接。然而，通过提供具有设备可被附属或连接多久的限制来降低订阅的价格，一些 M2M 网络运营商为 M2M 应用所有者提供激励机制。

网络运营商希望降低网络资源将需要一些机制来影响 M2M 设备的网络状态（连接的/附属的）。例如，一个选项是发送监督到 M2M 设备，该 M2M 设备显示发送数据之后设备应该做什么（例如，没有数据的 15min 后分离或者 3min 后断开）。发送监督到网络选择的移动设备将是类似的。一种替代方法是监督网络中的网络状态。例如，网络可能会在一个提前商定的每日最高接入持续时间之后断开 M2M 设备。应该指出的是限制存储在网络中的环境数据也有其他原因：终端用户可能有隐私问题，该隐私与他们的 M2M 设备的网络存储环境有关。例如，如果车辆管理应用的一个 M2M 设备保持连接以实现基于网络的连接，那么网络也将保持实现车辆

㊀ 注意，在演进分组系统（EPS）中，当一个移动设备通过 E-UTRAN 接入时，总会建立起默认连接。但是对于 M2M 应用，设备需要一直保持连接状态来保证其可到达性，而数据发送量极少，这时默认连接可能就不是很有效了。

位置跟踪的环境数据。由于这将引发一些汽车所有者的隐私问题，所以必须有这样一种车辆管理应用选择退出的方法。对于政府授权的应用，退出是没有可能的，例如道路收费或紧急呼叫，在网络中保持一个持久的移动管理环境将是不可能的。

6.3.3.2 避免网络信令

随着 M2M 通信的发展，大量网络信令和大量用户发送数据之间的速率是相对高的。对于 M2M 通信，调查如何降低大量的网络信令是有回报的。

降低大量网络信令的一个方法是对初始设备的信令（如附属请求、位置更新和连接请求）进行收费。M2M 应用所有者将尽可能高效的自动获得一个激励。然而，对于人对人的网络，信令不收取费用。在 CDR 处理中创建信令的 CDR 相比于将它保存在一个降低的网络信令中可能实际上生成更多的负载。

在移动网络中，低速移动设备的移动性管理信令可以被降低。一般情况下，移动性管理信令是定期重复的，以确保 M2M 设备仍然连接到网络上，虽然这种经常性移动管理信令的计时器值可被延长或者甚至设置为无穷大。在这种情况下，当 M2M 设备检测位置的变化时，仅仅执行移动管理信令。对于许多低的或者减少的移动性㊀M2M 设备，这意味着它们很少会产生移动性管理信令。

保持大量信令降低的另外一个简单方法是，当设备没有数据需要发送时尽可能保持其分离。不被重视的 M2M 设备也将不会创建任何网络信令。

对于频繁发送数据的设备，比如说每隔几分钟，保持连接开放可能是更有效的。连接和/或附属请求的频繁设置和拆除可能比保持实际需要的连接开放需要更多的信令。

对于频繁发送少量数据的应用，例如报警，信令需要附属和建立连接，然后可能会断开连接，重新附属相比于发送的少量数据代表一个很大的额外开销。毫无疑问，与信令相关的数据比实际的用户数据更多。对于这些应用的种类，最好的选择是附加信令中的用户数据。用户数据可能已经被包括在从 M2M 设备发送到网络的附属请求中。在这种情况下，认证是整体附属成功的程序的一部分，用户数据被转发到其目的地。

6.3.3.3 降低用户数据中的峰值

网络运营商需要度量其网络使用的峰值。最忙期间得到处理的任何额外通信意味着网络容量中的额外投资。另一方面，这意味着 M2M 通信是否可以被移动到非峰值，它几乎是免费处理的。在网络上运行的通信的边际成本在非常少的时间上有大量的空闲能力。

㊀ 自动售货机或打印机/复印机偶尔可以移动位置，但通常情况下是不移动的。对于这类设备，应当对其应用进行优化，使其降低或者减少流动性。

通过推动非时间敏感的应用到非高峰时段，定义在 3GPP 中的时间控制概念利用通信中的日常使用模式。例如，有许多应用，每天需要发送一次数据，但是当发送数据时它不是特别重要的。在这种情况下，通过确保在非高峰时期发送数据来节省成本。

在时间控制功能下，运营商和 M2M 应用所有者同意只能在一个特定的接入时间间隔内发送数据。再次，假设运营商通过降低应用程序的数据传输价格为 M2M 应用所有者提供一个激励，应用能够支持这种时间控制的限制。因为被给予的折扣，运营商希望监视 M2M 应用所有者是否确实已经设置了以下限制。

当一个接入请求，如一个附属或一个连接设置被一个在设备接入授予时间间隔之外的 M2M 设备接收时，请求可以被拒绝或者被接受，但是以不同的速率被控制。以较高的速率收费可能对运营商是优惠的，因为它仍然会产生收入。然而，缺点是收费解决方案变得非常复杂。改变收费速率意味着需要关闭现有的 CDR 来捕捉以旧速率和新速率发送的大量数据，对于以新速率发送的数据，需要打开现有的 CDR。需要生成和处理的额外的 CDR 可能会抵消在非高峰时间发送数据的成本优势。

对于运营商，非高峰期可能会随时间而改变。特别地，如果运营商将吸引大量具有大容量通信的 M2M 账户，那么非高峰时期可能真正开始填补。也可能是因为在日常模式或不同时区中的局部差异，局部的非高峰时间间隔是不同的。因此，时间控制功能允许运营商改变接入许可时间间隔，以适应局部的需求。M2M 设备和 M2M 服务器之间的通信需要更改后的接入许可时间间隔。拒绝（或接受）消息中接入请求的一个引发值可以被用来通知有关任何改变的 M2M 设备。

时间控制功能还包括一个禁止的时间间隔。在禁止时间间隔之间，所有的接入请求将被拒绝。这使得服务窗在 M2M 服务器上，不论本地网络环境，该服务器将不接收数据。禁止时间间隔不可以由网络运营商来改变。显然，禁止的时间间隔和接入许可的时间间隔不应重叠。

重要的是在接入许可的时间间隔内随机接入 M2M 设备。否则，在接入许可时间间隔之外，第一次尝试将启动所有在精确接入许可时间间隔开始处的通信，所有 M2M 设备必须停止其通信。例如，为了接入许可时间间隔的开始，M2M 设备可能添加一个随机时间偏移。

此外，有趣的是确定在接入许可时间间隔的末端会发生什么情况。如果一些 M2M 应用不设法得到它们在接入许可时间间隔内发送的数据，然后断开，那么它们将永远不会得到它们的数据跨越。然而，可以假设的是对于发送所有必要数据的 M2M 应用，定义的接入许可时间间隔是足够宽的。例如，在 M2M 应用的案例中，需要大约 5min 来发送数据，一个 1h 接入许可时间间隔可能是适当的。不同的 M2M 应用将被摊开在 1h 接入许可时间间隔上。这种情况下，在接入许可时间间隔

末端之后仍然存在的任何连接可以通过网络简单地被断开，因为它们违反了 M2M 应用所有者与网络运营商制定的协议（以同样的方式，当一个预付账户用完了信用时，电话呼叫被断开）。

3GPP 已经定义了作为一种机制的低优先通信的概念，以打击在特殊情况下由 M2M 通信引起的过载（见 6.3.7 节）。但是通过从网络使用更规则的高峰中分流 M2M 通信，作为低优先级定义的 M2M 设备和订阅也可以作为一种降低网络投资的方式工作。当一个低优先级的 M2M 设备在网络负载的一个高峰期尝试接入网络时，通过发回一个具有回退计时器的拒绝消息，它可以被推迟到下一个时刻。回退计时器失效之后仅仅是允许退回到网络上的 M2M 设备。因此，这种机制可以被用于阻止在额外峰值容量中投资，处理 M2M 通信需要该容量。

6.3.3.4　M2M 的单独网络

当 M2M 通信变得完全不同于人对人的通信时，实现一个完全独立的 M2M 通信基础设施是有利的。特定的 M2M 网络可以得到配置，并且可以专门缩放 M2M 通信，而其他网络可以保持人对人的优化。例如，除了有限的数据吞吐量，为了允许大量的订阅以及相关的环境数据，M2M 优化网络中的核心网络实体可以被缩放。同样，通过不赋予较高的吞吐量，而是在建立通信中保持一个非常低的延迟，M2M 通信的接入网络基础设施可能被做得很便宜。

在最极端的情况下，可以为 M2M 通信设置一个完全不同的接入和核心网络。然后为具有特定 M2M 网络的工作配置 M2M 设备。一个较少的极端案例是，M2M 和人对人的通信之间仍然共享接入网络，但是其中有一个 M2M 通信独立的核心网络。在这种情况下，接入网络必须能够识别 M2M 通信，以发送部分通信到专用的 M2M 核心网络。

6.3.4　M2M 的增值服务

在前面的章节中，我们已经看到 M2M 应用往往可以支持特定的限制，这是否会导致数据通信的一个较低价格。然而，除了一般的数据通信，M2M 应用通常也有特定的增值服务的要求。在 M2M 增值服务下，运营商可以制定吸引更多 M2M 应用所有者的基本连接服务，并且设置他们自身与只提供标准连接服务的运营商分离。

而适应于可能的运营商的成本降低，为不希望支付正常数据连接费用的 M2M 应用所有者提供一个较低的价格，额外费用将提供 M2M 增值服务。它们使运营商能够创造更多来自 M2M 服务的收入。

应当指出，M2M 增值服务不服务于 M2M 应用级别。M2M 增值服务涉及数据通信服务本身，而不是 M2M 设备和 M2M 服务器中的应用。M2M 增值服务的例子有：

- QoS 和优先级分化。
- 收费和订阅管理。
- 设备管理。
- 连接监控。
- 欺诈控制。
- 安全连接。

6.3.4.1　更高的 QoS 和优先级

不同的 M2M 应用将有不同的 QoS 要求。虽然许多 M2M 应用没有严格的 QoS 要求，并能以最大努力很好地处理 QoS，一些 M2M 应用比普通的数据服务有更高的 QoS 或优先权要求。运营商在其基于分组的网络中越来越多地提供 QoS 分化。这将体现许多 M2M 应用的附加价值。

M2M 应用的一些 QoS 要求依赖于被输送的介质类型。例如，因为其他视频流服务有 QoS 要求，那么以几乎相同的方式视频监控需要一个具有足够带宽的数据流 QoS。

在当前的人对人数据服务中，其他 QoS 要求更具体并且不那么频繁。其中一个是在延迟上的更严格的要求。一些远程控制应用要求一个比目前的标准更低的延迟，例如，至少在 2G 和 3G 移动网络中，控制发电机的一个反馈回路不可能有几百毫秒的往返延迟。固定网络将更适合得到一个足够低的传输延迟。然而，长期演进（LTE）的低延迟也为 M2M 应用提供了一个机会。鉴于 UMTS 中的延迟一般是 200ms 的规则，LTE 中的延迟通常低于 15ms。为了提供一个较低的延迟专门设计了 LTE，并且 LTE 提供了新的 M2M 应用的可能性，例如多用户游戏。

另一个例子是分配和保持优先级（ARP）。在网络拥塞的情况下，ARP 确定一个设备获取或保持连接的优先级。与不同业务量类别相反的是，ARP 工作在连接上，而不是工作在个人 IP 数据包上。例如，许多 M2M 应用可以处理一个比标准的互联网连通性更低的 ARP。这些 M2M 应用不是时间关键的，并且能够延缓它们的数据传输直到拥塞已经结束。但是有些 M2M 应用需要一个更高的 ARP。例如，即使在发生地震导致网络拥塞的情况下，地震传感器需要能够对地震发出报警。应用可以延迟其数据通信直到拥塞结束。携带心脏监测设备的患者也可能希望他们的设备有一个比其他业务数据稍微更高的优先级，这些数据业务存在于新年前夜的大量移动通信中。

数据连接的 QoS 被定义在 QoS 配置中。表 6-4 和表 6-5 给出了 UMTS 的 QoS 配置中的各种参数，也就是，不同的参数适用于不同的业务量类型。一个连接的 QoS 配置可以被设置在既定的连接上。订阅中的 QoS 配置决定最大的 QoS，一个特定用户的连接可以请求最大的 QoS。在固定和移动网络中，由 QoS 控制提供的可能性对于 M2M 应用似乎是足够的。

表 6-4 UMTS 中的 QoS 业务种类（由 3GPP 许可复制）

业务种类	会话种类	流种类	交互式的种类	背景
基本的特性	保存流的信息实体之间的时间关系（变化）	保存流的信息实体之间的时间关系（变化）	请求响应模式	目的地确实不希望某一时间内的数据
	会话模式（严格的并且低的延迟）		保存有效载荷内容	保存有效载荷内容

表 6-5 可适用于不同 UMTS 业务类型的 QoS 参数

业务种类	会话种类	流种类	交互式的种类	背景种类
最大的比特速率	√	√	√	√
交付命令	√	√	√	√
最大的 SDU 尺寸	√	√	√	√
SDU 格式信息	√	√	—	—
误 SDU 率	√	√	√	√
剩余的误比特率	√	√	√	√
错误的 SDU 交付	√	√	√	√
传输延迟	√	√	—	—
有保证的比特速率	√	√	—	—
业务处理优先级	—	—	√	—
配置/保留优先级	√	√	√	√
源统计描述符	√	√	—	—
信令指示	—	—	√	—
改进的配置/保留优先级	√	√	√	√

3GPP 中定义的一个特定的增值服务是优先报警信息。3GPP 已经定义了许多 MTC 功能，该功能可以使移动运营商降低成本，也意味着 M2M 应用所有者的一个限制。例如，随着 MTC 时间控制功能，M2M 设备可以只在一个特定的接入许可时间间隔内发送数据。预期的优先级报警消息能够覆盖这样的限制，这是必要的。因为优先级报警信息也覆盖了移动运营商的成本降低，所以优先级报警信息也将被收取相应的费用。

6.3.4.2　计费和订阅管理

在固定和移动通信中，为企业客户提供特定的计费和订阅管理安排是习惯性的。对几千名员工而言，具有移动订阅的一个企业用户将需要一个公司内部通信管理者的特定功能，例如，更容易地给新的员工分配电话号码。另外对于计费，特定的增加值已经被预见提供，例如，一个单一的计费涵盖所有的订阅以及各种报告能力。

一个 M2M 应用所有者最多可以有几百万订阅，而不是几千个订阅。这也将意味着有关订阅和计费的特定请求。对于 M2M 应用所有者而言，M2M 应用通常是其主要进程的一部分。这意味着对于具有相关于主要进程的 IT 流程，订阅管理需要整合。对于一个电力公司，为一个新的地址提供电力意味着在该地址上需要提供智能电表的 M2M 订阅。没有 IT 系统的整合，这将是一个不可能完成的任务。

消费电子行业中的 M2M 应用所有者有与订阅管理相关的其他要求。在一个特定国家中，他们经常制造设备，然后将这些设备运往世界各地。在消费电子设备中，如导航装置或摄像头，为了接入移动网络而需要的 SIM 卡通常是嵌入在设备中的。具有其 SIM 卡的设备将必须在工厂中进行测试。但是 M2M 应用所有者可能不希望支付这些类型测试的漫游费用。随后，M2M 设备进入供应链，直到它最终在世界各地的商店中。当设备仍然在仓库中时，M2M 应用所有者不希望支付订阅费用。只有当设备被出售给终端客户时，订阅应该被激活。所有具有 SIM 的这些特定 M2M 具体物流在工厂中就被嵌入到设备中，M2M 具体物流将需要特定的 M2M 订阅配置。

在理想的情况下，M2M 应用所有者希望进一步沿着供应链灵活地选择移动运营商。M2M 应用所有者宁愿在设备中放置一个“白色标签”SIM 卡。在后一阶段中，当确定在哪个国家出售设备时，应选择那个国家的一个合适的移动运营商。为了允许这一点，SIM 卡可以被配置在具有特定运营商的订阅细节（国际移动用户识别码（IMSI）、安全密钥和加密算法）“空中”。虽然运营商愿意引入这样的 SIM 卡的远程管理，因为它减少了他们的控制订阅，标准化开发正在 GSM 协会（GSMA）中进行，ETSI 智能卡平台和 3GPP 使 SIM 卡的远程管理成为可能。

6.3.4.3　设备管理

对于管理几十万 M2M 设备的一个 M2M 应用所有者，设备管理是一个非常重要的增值服务。维修所有的设备是非常昂贵的，M2M 应用所有者往往很少或没有可能获得物理的接入，例如设备。导航设备的一个生产商销售具有地图更新服务的设备。当制造商随后希望更新服务的网络地址时，已经销售给终端用户的导航设备也必须得到升级。另一个例子是一个远程控制的高速链路消息标志。维修这些类型的 M2M 设备往往是非常昂贵的，因为为他们获得的物理接入需要部分高速链路被关闭。M2M 应用所有者可以远程管理 M2M 设备中的设置，因此这样一个解决方案

深受欢迎。

在 M2M 应用水平上考虑设备管理，例如，在一个导航设备或一个通信水平上更新地图数据，更新 M2M 服务器的接入点名称或 IP 地址。通过 M2M 应用所有者本身，应用级的设备管理也可以被设置到 M2M 服务器，并且不被视为网络运营商的责任。网络运营商（一般的且非 M2M 设备）注重通信水平的设备管理。然而，为了给 M2M 应用所有者提供应用水平设备管理服务，网络运营商可以使用其现有的设备设施和网络管理。

应该特别注意在 M2M 设备的初始激活上的设备管理。在这种情况下，M2M 设备仍然需要获得将设备连接到 M2M 服务器的参数（例如，APN 和 IP 地址）。特别是在初始激活的情况下，网络运营商可以提供附加价值。

网络运营商在他们的处置上有现有的设备管理机制，这也被用于其他数据通信服务。移动网络运营商可以利用开放移动联盟设备管理（OMA-DM）框架［OMA DM］。固定的网络运营商可能使用框架，例如来自宽带论坛的 TR-069 框架［TR-069］。

6.3.4.4 连接监控

在正常的数据通信情况下，终端用户通常必须只监视一个设备和一个连接。然而，一个 M2M 应用所有者可能必须监视数以万计的设备和连接。此外，对于一个 M2M 应用所有者，获得到设备的接入往往是困难的或昂贵的。对于企业而言，M2M 应用所有者使用复印机的远程服务 M2M 连接，对复印机的上门服务简单地意味着工程师对用户服务呼叫的不便，但是对于使用海上监测风力机 M2M 应用的企业，M2M 设备的接入将真正成为一个主要的成本。一些 M2M 应用所有者将永远无法获得到 M2M 设备的接入；例如，一个销售导航设备的公司可能会得到一个用户的呼叫，该用户抱怨远程地图更新功能还不能使用。那么问题的远程诊断是唯一的选择。

监测 M2M 设备的连接状态往往是很重要的。对于一个安全报警应用，没有接收到警报是否表示一切正常，或这是否表示安全应用没有连接到 M2M 服务器，知道这一点很重要。例如，M2M 设备可能超出蜂窝的覆盖。

可以在应用级进行监测。当 M2M 设备和 M2M 服务器之间的连接有什么不妥时，在设备和服务器之间发送常规的诊断信息将检测 M2M 应用所有者。然而，对于许多应用，发送定期的诊断信息不是非常有效。对于报警应用，诊断信息将产生比实际用户数据更多的数据。特别是当数据连接被用作一个备份时，无需不断地发送数据，知道备份连接是否仍然可用是很重要的。

一个更好的选择是使用基于网络的设备状态监测。一种选择是监测定期流动性管理信令的接收。当接收到定期的流动性管理信令时，M2M 设备必须具有蜂窝覆盖并且能够连接网络。我们的想法是检测有关 M2M 设备连接的状态消息，该 M2M 设备没有产生许多附加数据或信令。

3GPP TS 22.368 中已经定义了一个 M2M 监测功能的要求。M2M 应用所有者可以定义哪些事件需要得到监测，例如，连接的损失，通用身份芯片卡（UICC）的切除或一个特定区域外的流动性。M2M 应用所有者还可以定义当检测到一个特定事件时需要做什么。在大多数情况下，将会通知 M2M 应用所有者。另外，如果检测到的事件是一个欺诈的指示，网络可能会自动限制到 M2M 设备的服务。

6.3.4.5　欺诈控制

许多 M2M 应用所有者拥有大量的 M2M 设备。此外，这些 M2M 设备往往是在公共场所，并且很容易受到欺诈或盗窃。比如，一个本地能源公司可能会使用 M2M 设备来切换或关闭路灯。在一个路灯结构中，M2M 设备可能位于某一个高处，但是对于公众，它们位于开放的和可接入的状态。有人可能会试图打开这样一个 M2M 设备，取出 SIM 卡并且为其他事情使用 SIM 卡。

对于 M2M 应用所有者而言，重要的是要尽早发现欺诈。通过基于网络的消息，网络运营商可以帮助指示欺诈行为。例如，在相同的应用内，如果一个特定的订阅突然发送比其他订阅的平均值多十倍的数据，那么可能会发生一些欺诈形式。该设备或 SIM 卡可能已经被盗，并且用于其他事情，例如，发送大量的个人数据。

第一道防线是实时（或接近）监测所有设备的使用。每当特定的订阅显示意外的行为模式时，M2M 应用所有者可以采取行动，例如，阻断这个特定的订阅。

其他方面可被用于表明有一些错误。例如，在具有低流动性（例如智能计量）的一个 M2M 应用中，不可预见的是 M2M 设备将突然从城市的另一边报告。如果 M2M 设备具有比预期更多的流动性，那么这是欺诈的另一个指示。

保护 SIM 卡不被滥用的另一个选择是限制特定设备的 SIM 卡使用。例如，这种关系可以基于 M2M 设备的国际移动设备标识符和软件版本（IMEISV）范围。然后 USIM 将只以设备的特定类型工作。通过一个类似的装置来取代该设备将是可能的，但是不可以将 SIM 卡插入不同类型的设备。

欺诈控制的第三个可能性是限制数据通信的可寻址的目的地。例如，限制 APN 和/或限制允许使用 M2M 设备的 IP 地址是可能的。

6.3.4.6　安全连接

网络运营商一般会确保其网络中传输数据的安全保护，例如，诚信、保密。例如，移动网络运营商可以为被传送到无线电接口上的数据加密。例如，在运营商的网络和客户的一个 M2M 服务器中，一般用一个 IP VPN 保护网关节点之间的接口。

然而，有些应用所有者需要额外的端到端的安全保护；例如，对于一个移动支付应用，在网络中的支付设备和 M2M 服务器之间可能使用一个安全的端到端 IPsec 通道。网络运营商不提供这种端到端的安全，这必须在应用级得到确保。

然而，[22.368] 的 3GPP 定义了一个与安全相关的 M2M 增值服务。运营商可以为具有密钥交换的应用所有者提供援助，端到端的加密需要密钥交换。与通用引

导结构（GBA）的使用类似［33.220］，在 UICC 和网络上的 SIM 应用之间的关联被用来产生设备和 M2M 服务器中的加密密钥。

6.3.5 编号、标识及寻址

M2M 的预期增长意味着有更多的 M2M 设备和更多的 M2M 相关订阅。所有这些设备需要编号、标识和寻址。问题是现有的编号、标识和寻址是否可以应付 M2M 的预期增长。这些足够长的编号和标识的结构可以满足数十亿的 M2M 设备和订阅吗？

3GPP［22.368］假设 M2M 比人对人通信多于两个数量级的设备和订阅需要得到标识和寻址。如果地球上有 6.5 亿人口，那么一个标识结构可以标识 10 亿订阅或设备，这些订阅或设备足够满足人对人通信的需求。3GPP 需求意味着一个标识结构应能保持 100×100 亿 =1 万亿特殊的标识。

6.3.5.1 E.164 编号

E.164 编号或电话号码中有一个紧急号码短缺。电话号码的规划和分配是通信监管机构的责任。然而，监管机构已表示，在一些国家中，M2M 通信的 E.164 编号将用完［ECC 153］。

用于电话应用的电话号码，其中 A 方“拨打”B 方的电话号码来表示呼叫的预期目标。在数据通信中，涵盖了大多数 M2M 通信，电话号码不是必需的[㊀]。为了确定数据通信的目标，一个 IP 地址似乎更合适。不过，通信网络中有许多地方，仍然依赖电话号码，例如：

- 在计费中-用于采集和传输计费数据的 CDR 包含数据号码。
- 在配置中-一个订阅配置记录在归属用户服务器中，该服务器没有电话号码被认为是无效的。将电话号码添加到订阅配置意味着订阅被激活。
- 在空中设备管理和移动通信中的 SIM 管理中，这常常意味着发送一个 SMS，需要一个电话号码来指示 SMS 的目的地。

图 6-8 所示的电话号码结构被定义在 ITU-T 建议案 E.164［E.164］中。

一个电话号码的最大长度是 15 位数字。通过 15 位数字，确定所有的 M2M 设备应该是可能的。即使我们消除了国家代码的最大三位数字，剩下的 12 位数字仍然可以确定每个国家中 1 万亿特定的电话号码。大多数国家中电话号码短缺的原因是电话编号较短。例如，北美编号计划使用 11 位数字的电话号码（包括国家代码）。此外，国家目的地代码被用于指示特定的地理区域或非地理号码的格式。这

㊀ 在 3GPP 的分组交换移动网络标准［23.060，23.401］中，电话号码不在任何连接设置或流动性管理过程中使用。电话号码只有在发送信息的时候才被传输，以便在控制与数据检索系统（CDR）中记录电话号码信息。

使得号码的分配效率较低。M2M 通信的大多数编号要求来自移动号码的范围。这种情况下，编号短缺是最紧迫的。在一些国家，可行的一个短期解决方案是在现有的 M2M 通信编号计划内定义新的编号范围。一个面向未来的解决方案是定义较长的 M2M 通信电话号码。人们更偏向于使用的更短、易使用的电话号码不适用于 M2M 通信，因此可以分配更长的电话号码。

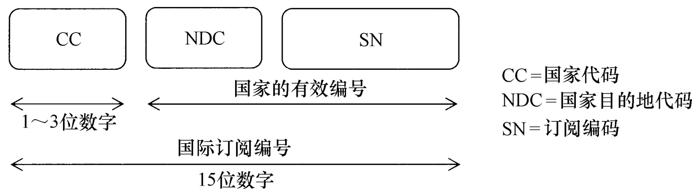


图 6-8　电话号码的 E. 164 编号格式

为了保持由 E. 164［E. 164］定义的最大编号长度内的安全性，为 M2M 通信的编号选择一个长度为 12 ~ 14 位数字的电话号码。通过所有的国际通信网络，应该安全地处理这样的电话号码长度。但是，增加电话号码的长度在大多数计费和配置的 IT 系统上将有一个显著的影响。运营商一般不乐于使用较长的 M2M 通信的电话号码。

另一个选择是在运营商之间重新使用一个 E. 164 编号范围，从而使国家中所有运营商允许使用一个特定的编号范围。在这种情况下，运营商之间不交换编号，也不支持这些编号之间的连接。对于许多应用，限制 M2M 应用所有者、网络运营商和 M2M 设备之间的电话号码使用没有问题。当事人以外的应用所有者不必到达 M2M 设备。M2M 应用涉及的多个当事人不仅仅为共享编号范围的解决方案工作。

在这些共享编号范围内不能提供号码便携性，因为一个特定的电话号码可能已经被分配在其他移动网络中。然而，号码便携性对于多数 M2M 应用已经不再是一个问题。M2M 应用所有者可能希望切换到一个新的网络运营商，但是改变电话号码仅仅是 M2M 应用所有者的一个内部问题。有关电话号码的改变不必通知其他当事人。

对于未来 M2M 服务的发展，正在提议 E. 164 编号的替代品。不需要为 E. 164 编号提供分组交换通信应该是可能的。在 3GPP［23. 888］和［22. 988］中研究消除依赖于 E. 164 编号的不同解决方案：

- 一种选择是为了不简单地使用一个电话号码（MSISDN），并且仅仅为了依赖订阅标识（IMSI）和 IP 寻址。对于运营商和订阅所有者之间的计费目的和供应，IMSI 是相当适合的。然而，在运营商和订阅所有者关系之外，由 IMSI 的使用引起了一些安全连接，这使得在方案中使用 IMSI 很困难，其中的第三方需要连接到 M2M 设备。然而，在许多 M2M 应用方案中，M2M 设备和 M2M 服务器中的订阅属

于相同的 M2M 应用所有者，因此也可使用 IMSI。为了保护移动网络和 M2M 服务器之间接口上的 IMSI，需要足够的安全性（例如 IP VPN）。使用现有的 IMSI 和 IP 寻址的好处仅仅是不要求定义新的标识；缺点是它不能处理所有的 M2M 应用方案。

● 在这种情况下，有多个当事人被卷入一个单一的 M2M 应用中，为了替代 MSISDN，一个新的标识具有优势；例如，当两个人想要玩一个直接的多用户游戏，他们需要能够识别其他游戏控制台，以便设置两者之间的通信。只使用 IP 寻址是不起作用的，因为游戏控制台可能改变了他们网络连接的位置和他们的 IP 地址。在这种情况下，IMSI 不是真正合适的，因为 IMSI 没有被设计成用作一个公共领域中的外部标识。为了替代 MSISDN 的作用需要一个新的标识符。一种选择是使用一个完全合格域名（FQDN）。一个 DNS 被用来存储属于该标识符的 M2M 设备的 IP 地址。另一种选择是使用一个 SIP URI。在这种情况下，一个 SIP/IMS 注册被用来存储 IP 地址和标识符之间的关系。取代具有一个新标识符的 MSISDN 的缺点是需要定义一个新的标识符结构。此外，一个新的标识符也意味着一个新的机构来分配这些标识符。建立这样的一个框架可能需要相当长的一段时间，包括相关的业务模型和管理问题，例如便携性要求。

6.3.5.2 其他标识符

其他标识符可能运行在具有许多预期 M2M 设备的空间以外。我们将关注三个相关的标识符：IMSI、IMEI 以及集成电路卡标识符（ICCID），看它们是否能够处理机器类通信的预测增长。

IMSI 被用在移动网络中以识别一个特定的订阅。IMSI 的结构如图 6-9 所示［23.002］。



图 6-9 国际移动用户识别码（IMSI）的格式

具有最少九位数字的一个移动用户标识号（MSIN），IMSI 结构能够保持一个移动运营商的至少 999999999 个订阅。但是如果我们假设 M2M 通信需要的标识符比人对人通信需要的标识符多 100 倍，那么具有超过 1000 万用户的一个运营商可能已经陷入了困境。有许多移动运营商目前有超过 1000 万用户，那么具有一个九位数字 MSIN 的 IMSI 可能不是足够长的。具有 10 位数字的 MSIN 有更多的空间，因为很少有运营商具有超过 1 亿的客户。然而，不能想当然地认为 IMSI 结构对处理 M2M 通信中的长期增长是足够长的。一个规避路线可能是分配多个移动网络代

码（MNC）到一个单独的运营商，因此对于具有大量 MNC 的运营商，最大数量的订阅将倍增。

IMEI 或国际移动设备标识符和软件版本（IMEISV）将被用于识别个人的移动设备。IMEI 的结构如图 6-10 所示［23.003］。

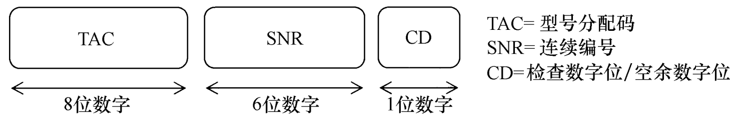


图 6-10　国际移动设备标识符（IMEI）的格式

IMEISV 的结构类似于 IMEI 的结构，一个两位数字的软件版本指示取代了校验数字，如图 6-11 所示［23.003］。

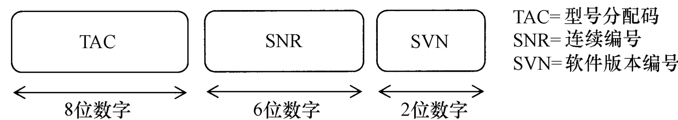


图 6-11　国际移动设备标识符和软件版本（IMEISV）的格式

型号分配码（TAC）识别一个特定的移动设备模型。SNR 是该型号所有设备的一个序列号。

具有一个 IMEI 的总数量为 10^{14} 的设备可以被唯一的标识，这似乎是满足需要的。然而，通过 TAC 大多数 14 位数字被占用。随着一个六位数字的 SNR，一个单一型号的设备的最大数目仅仅只有 100 万。一个特定的设备模型制造超过 100 万的单元是完全可以理解的。一个可能的规避路线是通过分配多个 TAC 到本质相同的设备型号。

ICCID 识别个人 UICC。在［E.118］中由 ITU-T 定义的 ICCID 的结构如图 6-12所示。

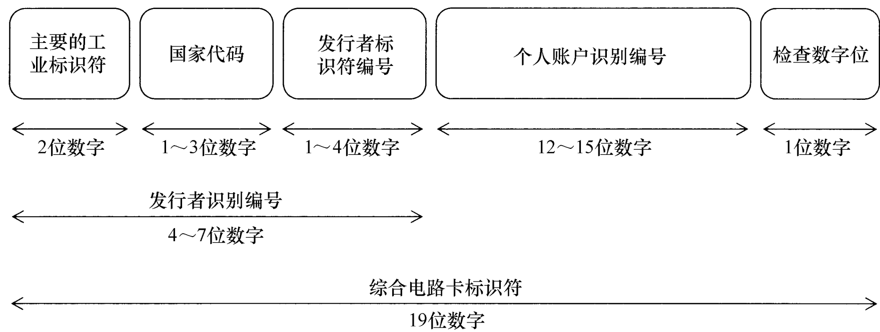


图 6-12　国际电路卡标识符（ICCID）的格式

对于个人 UICC 的每个发行者标识符编号，具有至少 12 位数字，ICCID 的结构似乎能够满足需要。

标识符的结构似乎是限制性的，M2M 的适应性是必须的。对于移动运营商，决定他们是否能够激活订阅的限制是上行的，这些订阅可以识别 IMSI，或者 IMSI 的一个扩展或者一个替换是否是必须的。更换或扩展 IMSI 都将在运营商通信基础设施和 IT 上产生很大的影响。IMEI/IMEISV 的结构和 ICCID 似乎产生的问题要小一些。

6.3.5.3 IP 地址

在世界范围内，正在被快速消耗的 IPv4 地址空间引起了巨大的关注。因此，大规模 M2M 应用的公共 IPv4 地址的使用不是一个真正的选择。另一方面，IPv6 提供了 3.4×10^{38} 这样一个精确的巨大地址量，M2M 应用将不再产生问题是不可能的。

理想情况下，M2M 设备和 M2M 服务器将获得所有的公共 IPv6 地址，在这种情况下，它们将共享同一个 IPv6 地址空间。如图 6-13 所示。

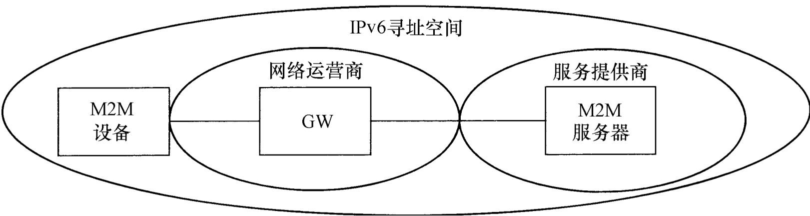


图 6-13 使用 IPv6 寻址的 M2M 通信方案

不幸的是，向着 IPv6 的迁移没有走到那一步。还有许多互联网目的地只可以通过 IPv4 地址达到。许多运营商和服务提供商对 IPv6 还没有完全准备好。因此，可以预见的是 IPv4 仍然会在 M2M 应用中被使用相当长的一段时间。通过使用私有的 IPv4 地址，IPv4 地址的短缺可被避开。一个典型的例子如图 6-14 所示。

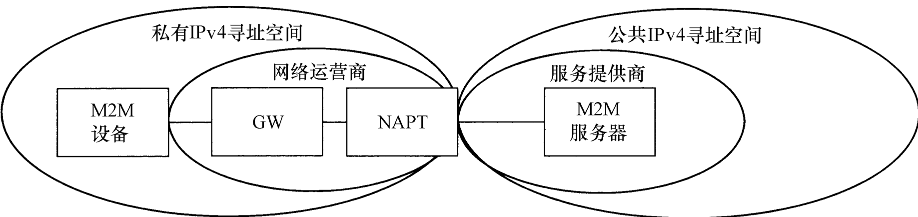


图 6-14 使用私有和公共 IPv4 寻址的 M2M 通信方案

在图 6-14 中，由网络运营商为 M2M 设备分配私有的 IPv4 地址。提供公共

IPv4 地址到所有这些 M2M 设备是对 IPv4 资源的一种浪费。网络地址和端口转换（NAPT）允许大量的 M2M 设备共享一个单独的公共 IP 地址。M2M 服务器被分配一个公共的 IP 地址。这使得来自不同网络的 M2M 服务器很容易接入，例如来自不同的固定和/或移动网络运营商。由于 M2M 服务器的数量是很低的，所以 IPv4 地址短缺问题要小一些。

NAPT 的一个问题是 M2M 服务器到 M2M 设备的寻址并不总是可能的。对于发送一个 IP 数据包到 M2M 设备的 M2M 服务器，NAPT 需要保持公共 IPv4 地址，在 NAPT 处端口号代表的 M2M 设备以及 M2M 设备的私有 IPv4 地址之间的关联。当 M2M 设备发送数据到 M2M 服务器时，建立了这个联系，并且该联系保持生存的时间长短与 M2M 设备保持发送数据的时间长短是相同的。要么 M2M 设备必须保持发送持续有效的信息，要么通过 M2M 设备必须启动一个新的数据会话，从而能够进行通信。M2M 服务器将必须触发（见 6.3.6 节）M2M 设备建立一个数据会话，在这种情况下，M2M 服务器希望与 M2M 设备发起通信。

NAPT 的另一个问题是标识符的映射。例如，在这种情况下，使用 FQDN 来更换电话号码，FQDN 和 IP 地址之间的一个映射通常保持在一个 DNS 中。如果 M2M 服务器需要通过 FQDN 发送信息到一个标识的 M2M 设备，它可以查找 DNS 中相应的 IP 地址。然而，具有 NAPT、IP 地址和端口号的一个特定的 M2M 设备可以改变每一个数据会话。

在 IPv6 寻址中，M2M 设备和 M2M 服务器可以存在于相同的 IP 地址域中，因此不需要 NAPT。尽管如此，IPv6 也可能存在于内盒（in-between box）之间，如数据路径中的防火墙。网络运营商将很可能不允许每个人发送 IP 数据包到 M2M 设备。网络运营商也可能希望防止内部的 IP 地址以及从外部可见的地址结构。这意味着 IPv6 寻址和与 NAPT 相关的 IPv4 有相似的问题；即，在 IP 寻址上通过没有另行数据交换和标识符映射的 M2M 服务器，M2M 设备的寻址也可以在 IPv6 中被广泛地实行。

当 M2M 服务器必须只工作在一个或多个网络中时，一个选择是对 M2M 设备和 M2M 服务器使用相同的私有 IP 地址域（见图 6-15）。一个好处是不需要 NAPT。如果 M2M 服务器不位于物理上相同的网络中（例如，它不属于网络运营商），在网关和 M2M 服务器之间设置一个通道（例如一个 IP VPN）。M2M 设备选择一个特定的网关，其中到 M2M 服务器的这条通道有一个终点。在一个分组交换移动网络中，这可以通过使用 M2M 服务器/应用的一个特定的 APN 来实施。私有 IP 地址可以通过网络运营商或通过拥有 M2M 服务器的服务提供商进行分配。当一个 IP 地址通过 RADIUS/Diameter 被分配给一个 M2M 设备时，RADIUS/Diameter 服务器可以通知 M2M 服务器。这样一来，当连接被建立时，M2M 服务器可以立即发送数据到 M2M 设备，即使 M2M 设备还没有发送任何数据。映射标识符到 IP 地址也没有问

题。具有私有 IPv4 寻址的方案并不总是合适的，因为它将限制置于可以被接入的 M2M 服务器上，但是它的简单性使得它成为一个有吸引力的解决方案。

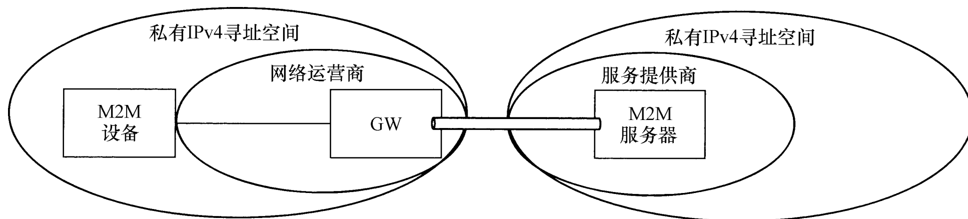


图 6-15 仅使用私有 IPv4 寻址的 M2M 通信方案

6.3.6 触发优化

许多 M2M 应用需要初始设备和网络的通信。在某些情况下，如果 M2M 设备可以启动 M2M 设备和 M2M 服务器之间的一个数据连接，这是足够的，但往往 M2M 服务器也需要能够启动数据连接。然而，固定和移动网络中的数据连接的建立一般是初始的设备。例如，GSM 和 UMTS 网络中数据连接的 PDP（分组数据协议）环境由用户设备（UE）进行设置。此外，大多数 IP 中间盒（middle box），例如防火墙和网络地址转换，对由设备发起的一个数据会话假设起作用。为了建立来自网络方面的一个连接，网络需要通知应该建立一个连接的设备。这个过程被称为触发。

现代 M2M 通信中的触发是共同的，虽然目前的触发形式中有一些问题，在这方面需要一些网络的改善，例如：

● 触发的一个特殊方式是建立到 M2M 设备的一个 CS 电话呼叫，这仍然是普遍的做法。M2M 设备不回应呼叫，而是把接踵而来的呼叫请求作为一个触发，并且建立一个到 M2M 服务器的数据连接。这种触发方式对运营商是特别没有吸引力的。M2M 设备需要 CS 网络中的功能，但它永远不会对那些 CS 资源产生收入，因为呼叫仍然没有应答。理想的情况下，M2M 订阅将只进行分组交换。

● 触发的另一种方式是使用 SMS 信息。当 M2M 设备接收一个（特别格式）SMS 时，它将作为一个触发。通过分组交换域发送 SMS 信息是可能的。这里的问题是发送一个 SMS 到定制的目的地需要一个电话编号。M2M 的电话编号有一个短缺（见 6.3.5 节）。

● SMS 的另一个问题是它是一个文本信息服务，现在这被“误用”为传输信令的一种方法。移动运营商正在为 SMS 增值服务引进设备，例如拦截垃圾邮件。此设备将对大量的触发信息进行缩放处理，这些触发信息基本上是信令信息，并没有受益于与文本信息相关的增值服务。

因为触发的重要性，对 3GPP 版本 11 获得最高的优先级是其中的一项任务。

应该进行更有效的触发，并且不依靠电话编号这应该是可能的。

6.3.6.1　触发的基础

当 M2M 服务器决定触发一个 M2M 设备时，它一般包括触发消息中的以下信息：

- 目标 M2M 设备的识别。
- 应用的识别。
- 一个请求计数器与该请求允许重复请求的检测相关联，对于具有其确认的请求相关性，允许应用取消请求。
- （任选）IP 地址（或 FQDN）和/或 UE 必须连接的应用服务器的端口号。
- （任选）一个迫切的请求指示。
- （任选）一个有效定时器，当不能够到达设备时，允许存储在网络中的触发拆除，例如，携带 SMS。
- （任选）需要发送区域中的触发。
- （任选）有限数量的特定应用信息，例如，在与 M2M 服务器建立通信之前，指示 M2M 设备来做一些事情。

M2M 服务器可以发送触发信息之前，需要确定向何处发送触发请求。3GPP 正在制定一个机器类通信网关（MTC GW），对于来自 M2M 服务器的控制信息，该网关将在移动网络中作为一个切入点。MTC GW 可以预先被配置在 M2M 服务器中，在这种情况下，M2M 服务器只与一个网络运营商进行通信。否则，M2M 服务器首先需要确定哪个运营商需要发送一个触发请求。根据设备 ID 或 IMSI，M2M 服务器应该能够找到正确的移动运营商网络。

图 6-16 显示了如何通过 MTC GW 发送所有的设备触发。只有当 M2M 设备和 M2M 服务器之间已经有一个积极的数据会话时，M2M 服务器可以通过简单地发送一个具有正确 IP 地址的 IP 数据包到网关 GPRS 支持节点（GGSN）或分组数据网络网关（P-GW）。

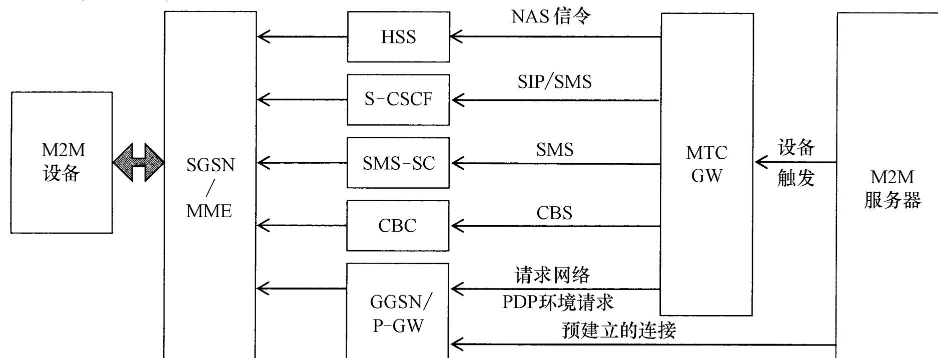


图 6-16　不同触发解决方案的概述架构

从 MTC GW 来说，有许多潜在的触发解决方案。[23.888] 中建议了许多解决方案。MTC GW 可被分配决定选择哪一个触发方法的作用，例如，基于来自网络的状态信息。但是，M2M 服务器也可以继续使用哪一个触发方法的决策点。M2M 服务器对 M2M 应用最了解，M2M 设备与该 M2M 应用相关，这些设备可以支持这种类型的触发方式。

在不同的连接状态中触发是有可能的。在［22.368］中，3GPP 规定在一个连接状态和一个非连接状态中需要触发，这些触发有时连接有时非连接。当 M2M 设备处在一个连接状态中时，现有的连接可以被用于连接 M2M 设备。据推测，M2M 服务器知道 M2M 设备的 IP 地址，并且用于中间盒没有问题。然后，该 IP 分组可被传递到 M2M 设备。在某些情况下，M2M 设备处在一个连接的状态中，在这个意义上，它有一个逻辑数据连接（例如 PDP 环境,）但是没有一个无线电资源连接。在这种情况下，现有的寻呼方法［23.060，23.401］可以被用来重新建立无线连接和投递 IP 分组。

当安装 M2M 设备时，不具有数据连接，触发可被用来设立来自 M2M 服务器的通信。此外，当 M2M 设备得到连接时，但是 M2M 服务器没有 M2M 设备的一个可用的 IP 地址，M2M 服务器需要触发 M2M 设备。

此外，当 M2M 设备没有被连接时，能够触发 M2M 设备是有用的。一般情况下，非连接暗示 M2M 设备是无法到达的。没有被连接到的网络，非移动性管理环境在该网络中是可用的，并且在哪里寻呼 M2M 是不知道的。但是当通过其他方式知道位置时，触发设备是可能的。例如，如果 M2M 设备是静止的，M2M 设备的位置可能被存储在归属用户服务器（HSS）中。另外，M2M 应用可能知道 M2M 设备的位置。例如，一个自动售货机公司在其 IT 系统中具有信息，该 IT 系统处在它的自动售货机所在的位置。M2M 服务器可以使用该信息，以指示网络在该位置广播一个触发消息。有关 M2M 设备的位置信息也可以来自该事件中的 M2M 设备本身，M2M 设备每次感觉它的位置已经移动（例如，一台复印机正被移动到一个不同的建筑）就会报告它的位置。

触发非常低功耗的 M2M 设备引起了一个特定的问题。非常低功耗的 M2M 设备不希望一直监听网络，因为这需要能量。这些 M2M 设备只是偶尔打开来监听网络。问题是为了触发非常低功耗的设备，当它们正在监听网络时，它必须是已知的。如果当它们不监听时发送一个触发，该触发将不会被接收。另一种方法是使用一个存储转发机制，当 M2M 设备再次注册到网络时，该机制将发送触发消息。例如，一个 SMS 将被存储在网络中，并且当分离或关闭之后的 M2M 设备再次连接到网络时该 SMS 将被传送。

出于安全方面的考虑，触发经常只被限制到经授权的来源。一个触发会导致 M2M 设备建立一个到 M2M 服务器的连接。M2M 应用所有者将必须为发送在连接

上的数据付出代价，因此如果一个 M2M 设备被一个未经授权的来源错误地触发，它仍然可能会花费 M2M 应用所有者的钱。甚至更糟的是，M2M 设备的触发是否是由恶意的原因引起的。例如，多次触发 M2M 设备可能会导致服务攻击的一个拒绝。MTC GW 可以验证触发请求源，以确保该信息源被授权发送触发到特定的 M2M 设备。

在［23.888］中，描述了触发一个 M2M 设备的许多不同机制。触发机制中还没有被选择的 3GPP 将会正式得到标准化。在所有的可能性中，许多解决方案将被标准化，因为每个不同的触发机制都有长处和不足。这里有五个不同的触发机制：

- 使用移动终止的 SMS 触发。
- 使用 IMS 信息触发。
- 使用小区广播触发。
- 通过 HSS 和非接入层（NAS）信令触发。
- 通过网络请求的 PDP 环境建立触发。

6.3.6.2　使用移动终止的 SMS 触发

图 6-17 显示了如何通过由 MTC GW 转发到 SMS 服务中心（SMS SC）的 M2M 服务器发送触发。由此看来，该程序几乎是标准的移动终止 SMS 程序［23.040］。主要的区别是在正常的 SMS 程序中，一个 MSISDN 被用作设备标识符。在 M2M 通信中，无论是 IMSI 还是一个 MSISDN 更换将被使用。这意味着 SendRoutingInfo-forSMS 程序的一个更改。

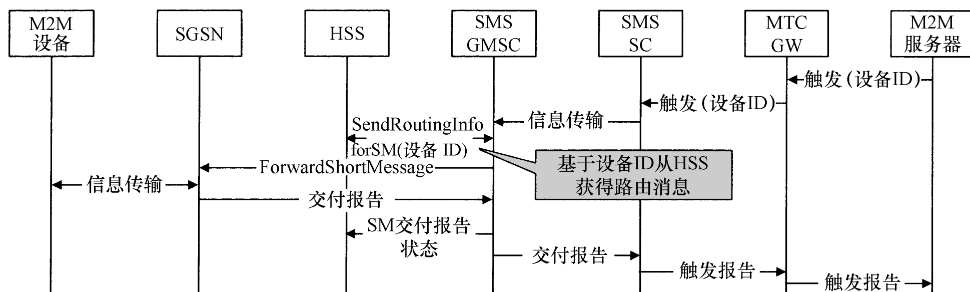


图 6-17　使用移动终止 SMS 程序的触发

使用移动终止 SMS 触发的优点是，对现有的网络和标准不需要做许多改变。其缺点是，它没有寻址一种改进 M2M 触发解决方案的所有要求。即使可以回避依赖 MSISDN，仍然有一个问题，就是防止未经授权的 SMS 信息是很困难的。一个恶意的发送者可以使用一个标准的内部运营商接口，以发送未经授权的 ForwardShort-Message 消息到他们期望可以到达的 M2M 设备的目的地 SGSN。由于许多 M2M 设备不是移动的，因此发现没有来自 HSS 请求路由信息的 M2M 设备有一个相当好的

机会。区分这类未经授权的 ForwardShortMessage 信息和真正接收到的 SMS 消息是非常困难的。

6.3.6.3 使用 IMS 信息触发

在 LTE 中，由于使用 IMS 实时信息实现短信，所以没有固有的 SMS 支持。因而在 LTE 中，基于 SMS 的触发可能是困难的，另一种可能是使用 SIP 信息。图 6-18 显示了 IMS 信息如何可以被用到一个 M2M 设备。M2M 设备首先需要在 IMS 中注册，以便能够接收 IMS 信息。MTC GW 被视为一个 IMS 应用服务器和 M2M 设备的注册，服务呼叫中的会话控制功能被转发到 MTC GW。当一个触发到达 MTC GW 时，通过 IMS 服务控制与 S-CSCF 的接口，为 M2M 设备开始一个 SIP 信息。

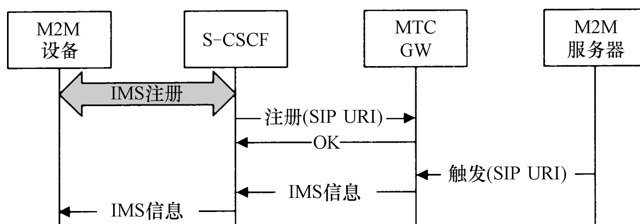


图 6-18 使用 IMS 信息触发

这种解决方案的缺点是 M2M 设备需要维护一个 IMS 注册。这需要 IMS 凭据和身份验证，再现重新注册，S-CSCF 功能等。M2M 应用的沉重负荷可能只发送和接收少量的数据。这种解决方案的优点是它需要对现有的标准作很少的更改。

6.3.6.4 使用小区广播触发

图 6-19 显示了使用小区广播触发。此解决方案隐藏的假设是 M2M 服务器知道 M2M 设备所在的区域。一个有关区域的触发请求被发送到 MTC GW，它将其转发到小区广播中心（CBC）。由此看来，小区广播［23.041］的标准程序被用来广播指示区域内的触发信息。M2M 设备监听广播信息。如果发送到触发信息中的识别与其自己的识别之间有一个匹配，那么 M2M 设备将建立一个到 M2M 服务器的连接。

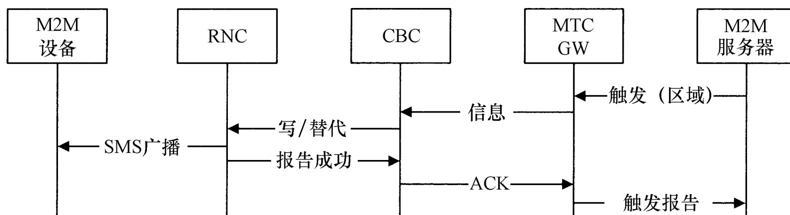


图 6-19 使用小区广播触发

被用在触发信息中的识别可以是任何的应用级识别；它对移动网络是完全透明的。例如，一个智能计量应用可以使用电子仪表的序列号。标识符也可以识别一组 M2M 设备。例如这允许一个有效的方式来触发一批 M2M 设备进行一个软件升级。然而，应当注意的是，确保没有太大数量的 M2M 设备会同时连接到 M2M 服务器。触发信息的响应应该随着时间的推移传播。

M2M 服务器确定在哪个区域广播触发信息，以同样的方式来完成小区广播。为了减少广播渠道上的容量需求，理想情况下，触发信息应该在一个有限的区域内被广播。对于一个非移动的 M2M 设备，在一些小区中广播就足够了。然而，在一个较大的区域中广播触发信息是可能的；例如，在一个被报告偷窃的车辆中，为了触发一个跟踪装置，它将比一个较小的区域中广播花费更多的成本。对于 M2M 应用所有者，小区广播可能是触发 M2M 设备的一个有效的方式，而对于移动运营商，它提供了收入的一个额外资源和投资在小区广播基础设施上的回报。

通过小区广播的触发也可以为不被重视的 M2M 设备工作。这将需要 M2M 设备继续监听被分离的广播渠道。虽然处于断电状态的分离设备的这个概念显然是过时的，但是为了实现这一目标，移动设备标准将需要更改。

6.3.6.5　通过 HSS 和 NAS 信令触发

图 6-20 显示了使用现有 NAS 信令触发的一个信息序列。这个概念隐藏的思想是，在 M2M 设备和网络之间的现有信令上，触发信息可以是附带发生的。

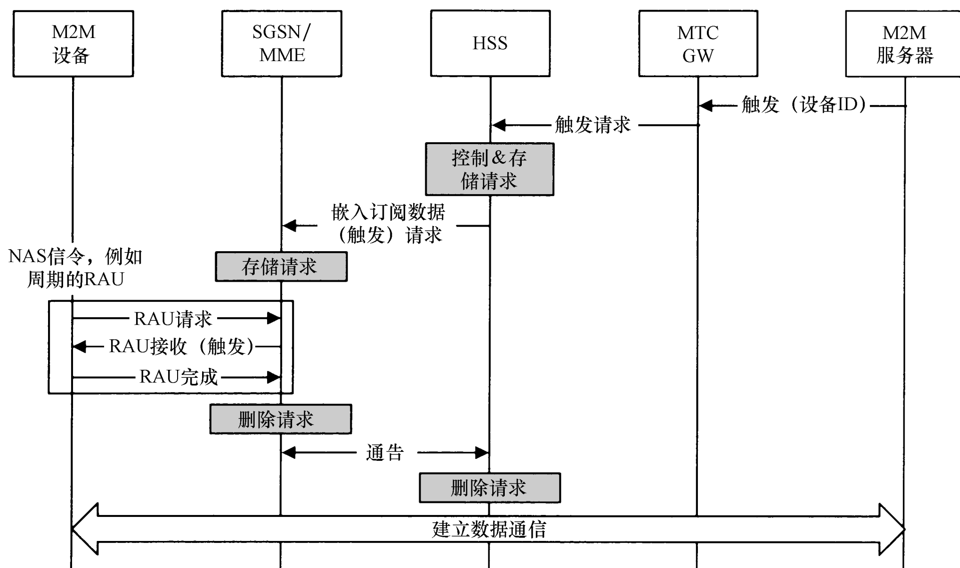


图 6-20　通过 HSS 和 NAS 信令触发

通过 MTC GW 发送触发请求到 HSS。HSS 存储该请求，并且当 M2M 设备被安装时，在一个添加用户信息中发送该请求到 SGSN 或 MME，其中的 M2M 被注册。当 M2M 设备下一步对 SGSN/MME 发送信号时；例如，对于一个周期性路由区域更新，SGSN/MME 依附 M2M 设备响应中的触发信息。当触发信息被成功地接收时，触发请求将由 SGSN/MME 和 HSS 删除。在 M2M 设备还没有得到安装的情况下，HSS 将存储触发请求，直到下一次 M2M 设备重新连接到网络。

这种机制的好处是不需要横跨在无线接口之间的额外信令来传输触发信息。这种机制的存储和转发性质既有优点也有缺点：触发信息是否已经到达 M2M 设备，没有直接的反馈，但是“发射后不管”机制意味着 M2M 服务器不必跟踪接收到的和需要重新发送的触发信息。

6.3.6.6 通过网络请求的 PDP 环境建立触发

图 6-21 描绘了五个触发机制的最后一个。在［23.060］中，很久以前就指定了该网络请求的 PDP 环境激活程序。唯一新的方面是从 MTC GW 到 GGSN 的连接请求。现有的网络请求的 PDP 环境激活过程还没有被一个信令信息启动，但是由设备的一个 IP 数据包的收据启动。

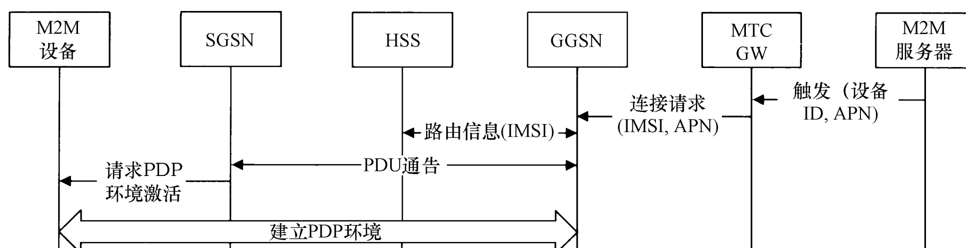


图 6-21 通过网络请求的 PDP 环境激活触发

HSS 中发现的路由信息，以确定 SGSN 在 IMSI 的基础上发送触发信息。这是如何标准化网络请求的 PDP 环境激活，但是不经常实施 HSS 的这个基于 IMSI 的查询。为了查询 HSS，使用 MSISDN 的一个新设备 ID 更换也可能是一个选择。

6.3.6.7 触发机制的结论

在 3GPP 中有许多不同的触发机制方案。目前尚不清楚的是，为规范的标准化规格将选定这些机制中的哪一个。最大的可能是解决方案的一个混合物将被标准化。M2M 服务器可以选择最适合应用和 M2M 设备的那个触发机制。

6.3.7 过载和拥塞控制

从长远来看，预计 M2M 设备将比个人通信设备多两个数量级。直接与移动网络运营商相关的 M2M 设备的数量已经很显著，并且有各种情况，其中在移动网络

中大量的 M2M 设备已经遭受了显著的拥挤。由 M2M 设备造成的过载和拥塞是所有同时接入网络的 M2M 设备同步行为的主要结果。过载和拥塞同样可以由移动运营商自己的 M2M 订阅和漫游在一个运营商网络上的 M2M 设备造成。在后者情况下，通信模式可能比预测的要少得多。例如，可能造成 M2M 相关的信令拥塞和过载：

- M2M 应用在精确的同步时间间隔上生成重复的数据传输（比如，精确的每一小时或半小时，见图 6-22）。

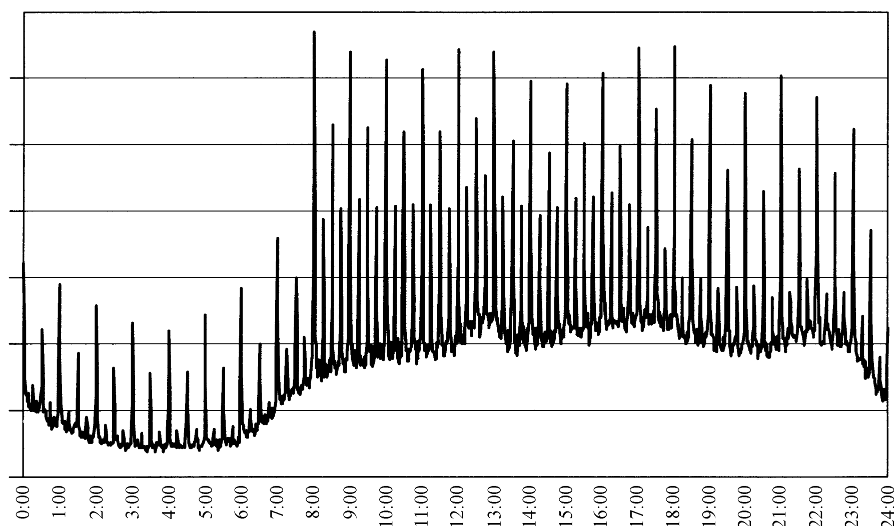


图 6-22　从 M2M 应用（在一个 RADIUS 服务器上加载）
接入的同步数据示例（由 TNO 许可转载）

- 为了附加/连接一次，一个外部事件触发大规模的 M2M 设备，例如，停电之后，大量的计量设备几乎同时变得活跃。
- 大量的传感器都触发一次。一个特别的例子是监视一座桥的一个应用。当一辆火车经过这座桥时，所有的传感器几乎同时传输监控数据。同样的事情也发生在大雨时的水文监测中，以及当入侵者的闯入时的建筑监视中。
- M2M 应用和/或 M2M 服务器中的一个故障，例如，当 M2M 服务器不承认接收到由 M2M 设备发送的数据时，所有的 M2M 设备保持重新发送其数据。
- 随着一个基站中断，许多 M2M 漫游设备失去网络覆盖。这些 M2M 设备将全部同时漫游到竞争移动网络的另一个位置。

一些过载和拥塞情况可能会经常发生，而另一些是非常罕见的事件。从 M2M 应用接入的数据同步峰将必须被视为一个正常的情况，因为其他应用不应接受 M2M 应用的行为。同样，当一个单一的 M2M 应用引起拥塞时，其他 M2M 和非

M2M 应用不应该受到影响。然而，也有更不寻常的事件，例如网络中断，地震或其他灾害情况。在这样的事件中，大规模数量的 M2M 设备的组合有一个可能性，这些 M2M 设备尝试接入网络（例如，由地震触发消防/防盗报警器），并且网络具有减少网络中断或灾难的能力。这些是特殊的情况，其中的目的是为了防止只具有优先级和被保证的紧急服务功能的一个完整网络崩溃。

M2M 拥塞和过载情况主要涉及控制平面的拥塞和过载。虽然 M2M 应用可能会产生非常高的用户平面数据负载是可以想象的，但是大多数 M2M 设备只发送有限数量的用户数据。M2M 相关的拥塞和过载可能影响移动无线网络部分（也就是说，当许多 M2M 设备需要在一个特定的区域中几乎同时传输数据时）和/或移动核心网络，例如，如图 6-23所示，大量的计量设备需要几乎同时向相同的 M2M 服务器传输数据。

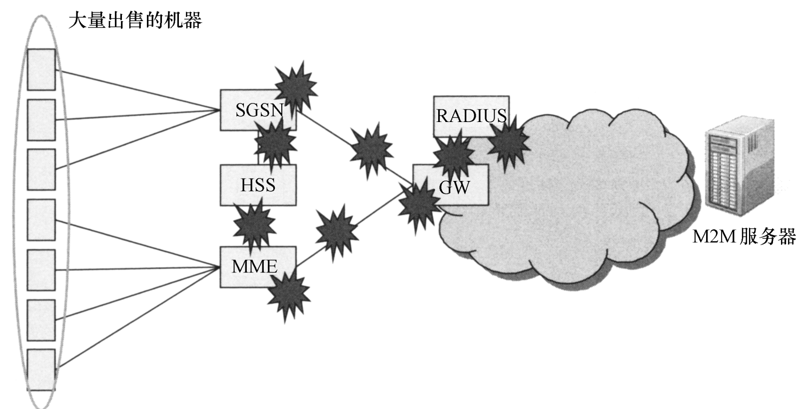


图 6-23 移动核心网络中的 M2M 信令拥塞（由 3GPP 许可转载）

移动核心网络节点可能遭受 M2M 相关的信令拥塞包括：

● 所有 PS 域控制平面节点和网关。随着大规模的连接请求，该服务控制节点（SGSN/MME）大体上是脆弱的。随着数据的连接请求，SGSN/MME 也是脆弱的，因为这个节点的每个连接请求都有一个比较大的负载。网关节点（GGSN/PGW）是特别脆弱的，因为 M2M 应用程序通常使用一个专用的 APN，该 APN 可能被终止在一个 GGSN/PGW 上。然后特定应用程序的所有连接请求将必须要由一个单一的 GGSN/PGW 处理。M2M 设备可能只在一个有限的区域中同时尝试信令交互。这意味着，信令拥塞可能发生在一个或几个特定的信令链路，并且在网络节点上没有出现整体拥塞。

● CS 域中的 MSC/VLR。由于移动运营商需要通过 SMS，以及 PS 域 SMS 的有限的有效性来配置设备，大多数现有的 M2M 设备需要尝试接入 CS 域。大量的 M2M 设备可能会尝试同时注册在 CS 网络上，在这种情况下，本地竞争网络会

失败。

对于在一个位置中的移动网络运营商，必不可少的是保护他们的网络免受潜在的 M2M 相关的过载，以至于不降低 CS 或 PS 服务的质量，这些服务目前提供给他们的用户，例如，语音呼叫或 SMS。

6.3.7.1　过载和拥塞控制机制

当过载状况涉及来自多种 M2M 应用和设备的一个不正常的使用时，为了保护移动运营商网络免受彻底的崩溃，一般的过载和拥塞控制机制是必要的。保护机制的目的在于管理独立于其他“传统”设备的所有 M2M 设备/应用的网络负载，并且保护机制会影响所有的或许多的 M2M 应用。

为了管理来自一个特定 M2M 用户的一个特定的 M2M 应用或 M2M 设备的网络负载，特定应用程序拥塞控制机制是必须的，例如，为了保护移动运营商网络免受一个较差的行为应用。因为由一个应用造成的拥塞不应该对其他（M2M）应用造成不利的影响，所以保护机制专门针对没有限制的非 M2M 业务量或来自其他 M2M 应用的业务量的应用，这些 M2M 应用不会引起问题。对于标识特定的，大规模的 M2M 应用，专用的 APN 或 M2M 组标识符是可能的办法。

拒绝连接或连接请求不应该导致一个 M2M 设备立即重启相同或不同网络内的相同请求。直到一个回退时间之后，该网络应该能够指导 M2M 设备不展开类似的请求。这个回退时间也可以被用来指示具有循环应用的 M2M 设备改变它们的附加/连接请求时间。

在许多情况下，M2M 设备将被用作一个网络运营商和一家大型的跨国公司之间一部分的连接。通常情况下，一个跨国 M2M 用户，如一个汽车制造商，将希望只与一个或多个移动网络运营商有一个合同，不管各个国家使用的 M2M 设备。这不可避免地导致很多 M2M 设备大部分时间漫游。当许多 M2M 设备是漫游的并且它们的服务网络出现故障时，所有这些 M2M 设备将同时移动到本地竞争网络，潜在的过载网络还没有失败过。需要机制来提供保护，以免受失败网络的这种多米诺骨牌效应。

下面的功能已被定义在 3GPP 版本 10 中，以保护移动网络免受 M2M 相关的信令拥塞和过载。虽然在 M2M 方案的主要动机和使用情况下，这些特点是普遍适用的：它们已被指定在一个通用的方式中，允许它们被任何移动设备使用。通过设备的运营商配置或设置订阅数据，这些功能可以被激活或失效。

6.3.7.2　移动设备的网络过载控制配置“低接入优先级”

使用容忍延时的 M2M 应用的 M2M 设备可以由后续配置得到配置，该后续配置是移动运营商和 M2M 用户之间的“低接入优先级”待定协议。

对于移动台发起的服务，一个 M2M 设备为低接入优先级信号配置其“低接入优先级”到无线资源控制（RRC）间的无线接入网络，连接建立程序和 NAS[㊀]信令流程间的 CS 和 PS 核心网络（MSC、SGSN 和 MME），例如，为 CS 或 PS 核心网络注册，或请求一个数据连接的建立。在数据连接建立期间，PS 核心网络节点（MME 或 SGSN）提出了连接建立请求信息中的低接入优先级指示，该信息发送到网关节点（服务 GW 和分组数据网络 GW）。

图 6-24 描述了由一个移动设备（UE）启动的一个附加程序的高层视图，该移动设备配置了低接入优先级，只表示 RRC 连接的设置（即无线信号连接），附加程序的启动面向 MME，并且相应的数据连接的建立面向 P-GW。

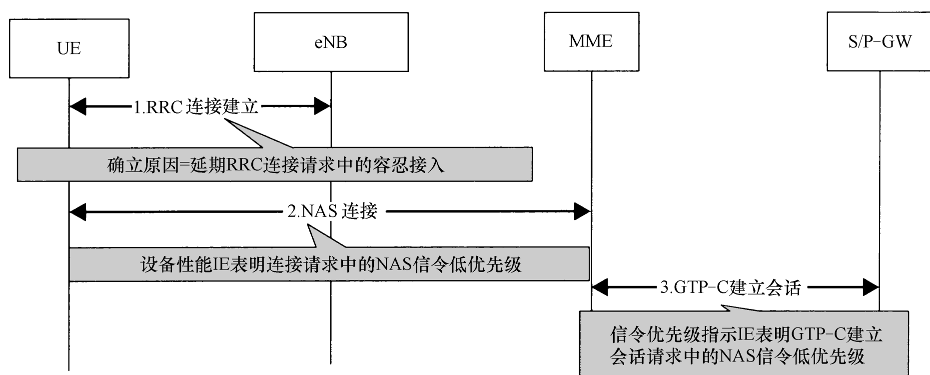


图 6-24　由低接入优先级配置的 UE 的附属程序

低接入优先级指示可以使无线接入网络节点（RNC/eNodeB）和核心网络节点（MSC、MME、SGSN、SGW 和 PGW）决定是否接受 RRC 连接设置，或根据当前网络负载的 NAS 请求。在没有低接入优先指示器拒绝请求信息之前，经历一般过载的无线接入网络和核心网络节点可能会拒绝来自配置有低接入优先级的移动设备的请求。经历一般过载的一个 MME 也可能请求无线接入网络，以限制接入从低接入优先级的配置设备到网络，通过发送一个“过载开始”消息到 eNodeB 的一个选择。如果有必要，为了拒绝由设备启动的 RRC 连接请求不配置低接入优先级，MME 也可能进一步要求无线接入网络，即为了拒绝所有的 RRC 连接请求，该请求赞成非紧急和非高优先级发起的移动服务。

当请求这样做时，eNodeB 拒绝由配置有低接入优先级的设备启动 RRC 连接建立请求，对于被拒绝的网络，在进一步请求期间具有一个扩展的等待计时器。

㊀ 网络连接式存储（NAS）的信号是直接在移动终端和核心网络节点之间发送的，信号在无线接入网络中穿梭自如。

当 MME 已经恢复时，MME 希望对低接入优先级配置的移动设备增加其负载，MME 将一个“过载停止”消息发送到 eNodeB。

图 6-25 显示了整体的过程。

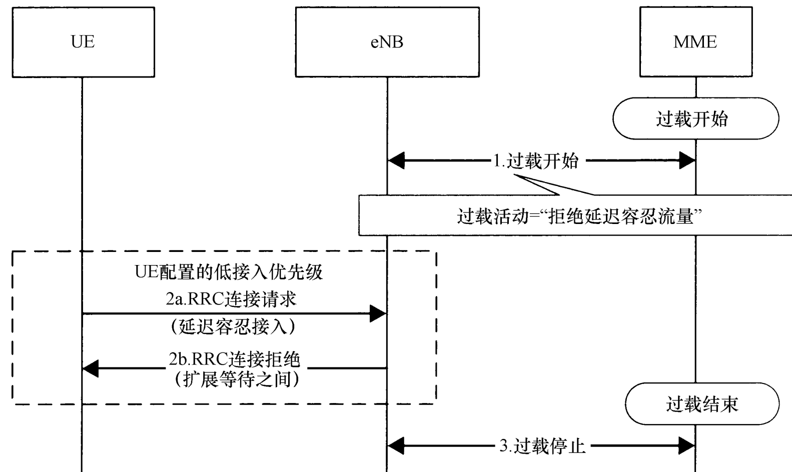


图 6-25　限制网络接入到低接入优先级配置的 UE 的过载程序

对于经历一般过载的一个 SGSN，类似的机制也已经被定义。在一个过载情况下，一个 SGSN 可以请求无线网络控制器来限制配置有低接入优先级的移动设备的负载。在这样的情况下，无线接入网络拒绝连接请求。

设备的相应子类别的 RRC 连接机构，具有一个适当的定时器值限制进一步的 RRC 连接请求。

6.3.7.3　通用核心网络移动性管理拥塞控制

在一般性过载条件下，一个 MME 或 SGSN 可能会拒绝来自移动设备的移动性管理信令请求（即，连接，跟踪区更新或路由区更新请求）。当拒绝一个 NAS 请求时，MME 或 SGSN 可以提供具有一个移动性管理回退计时器的设备，在此期间，移动设备将无法启动除了高优先级业务、紧急服务以及移动终止服务以外的任何进一步的 NAS 请求。

类似的程序也已经被定义为 CS 域。在流动性管理期间，一个 MSC/VLR 也可以执行拥塞控制，也就是说，经历拥塞的一个 MSC/VLR 可能拒绝由一个移动设备启动的一个位置更新请求或 IMSI 附加消息，排斥反应是由于拥塞，具有一个指示和 CS 域的一个特定的移动性管理回退计时器。当流动性管理回退计时器正在运行时，不允许设备启动任何移动性管理程序，除了优先/紧急服务和移动终止服务。

为了避免大量移动设备（几乎）同时启动递延请求，MSC/VLR，MME，和 SGSN 应该分别选择移动性管理回退计时器值，以致延缓请求是随机的。

如果由移动设备发出信号，适用于移动性管理拥塞控制的决策可能考虑低接入优先级指示。

6.3.7.4 在空闲模式中，M2M 设备收到的下行低优先级业务量的选择性节流

上面给出的机制可以由被控制或节流的移动设备发起上行链路信令。也有一个机制来保护 MME 免受巨大的同时发生的下行链路业务量，该业务量从 M2M 服务器转发到具有既定的低优先级数据连接的设备。当一个下行链路用户平面分组到达待机模式中的一个移动设备的服务 GW 时，即使有一个逻辑数据连接，移动设备将需要被呼叫。这个寻呼过程由 MME 处理。经历过载的一个 MME 可能限制信令过载，因为下行用户平面分组，服务 GW 正在产生。这个机制如图 6-26 所示。

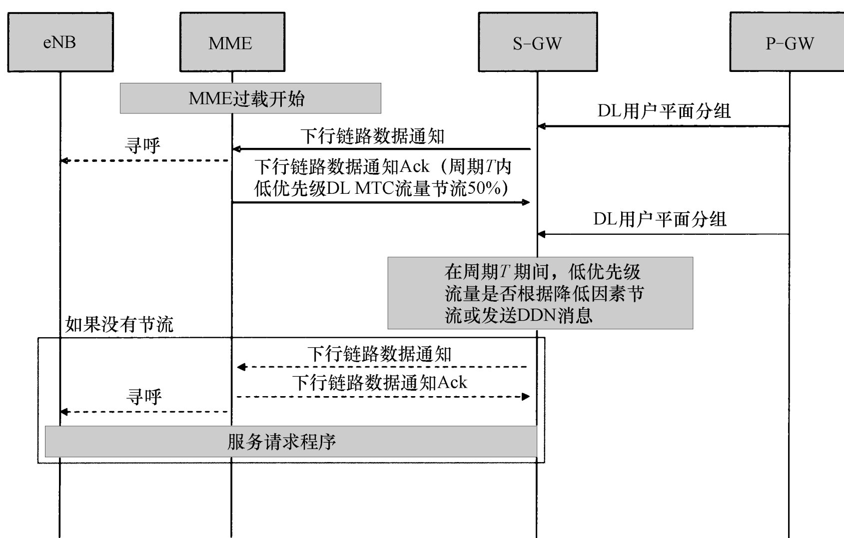


图 6-26 空闲模式中移动设备收到的下行链路低优先级业务量的节流

当服务 GW 接收到待机模式中的一个移动设备的一个下行链路用户数据平面分组时，它将为 MME 发送一个下行链路数据通知。对于低优先级业务量或进一步的卸载 MME，MME 可能会拒绝这样的下行数据通知请求，根据节流因子和一个特定的持续时间，它可能会要求服务 GW 有选择地降低下行链路数据通知请求的数量。

在承载的分配和保留优先级（ARP）水平和运营商策略的基础上（即被视为优先级或非优先级业务量 ARP 水平的运营商的配置），服务 GW 和 MME 确定一个承载是否与低优先级业务相关。MME 从下行链路数据通知信息中的服务 GW 处接收 ARP 优先级水平。

当节流时，对于在节流因子的比例中被认为是非用户平面连接（即服务 GW 环境数据不指示任何下行链路用户平面通道）的移动设备，服务 GW 放弃其所有

的低优先级承载上接收到的下行链路数据，并只为非节流承载发送一个下行链路数据信息到 MME。

服务 GW 在限制期限到期后恢复正常的操作。

6.3.7.5 特定应用的拥塞控制

特定应用的拥塞控制是一种保护机制，为了避免和处理与一个特定的 APN 相关的信令拥塞，即它只针对使用特定的 APN 的 M2M 应用。分组数据网络 GW 可以检测 APN 相关的拥塞，并且根据标准开始和停止执行过载控制，如：

- 每个 APN 的活跃承载的最大数量。
- 每个 APN 的承载激活的最大速率。

当执行过载控制时，分组数据网络 GW 拒绝数据连接建立请求。在响应中，它可以包括一个会话管理回退时间，表示 MME 应该多久避免发送后续的数据连接建立请求。一旦收到来自分组数据网络 GW 的拒绝，如果任何 APN 可以拒绝来自移动设备的数据连接请求，MME 可以选择一种交替的数据网络 GW 服务。

一个 MME/SGSN 可以检测与一个特定 APN 相关的会话管理拥塞，并且由监控标准开始和停止执行基于 APN 的会话管理拥塞控制，例如：

- 每个 APN 的活跃承载的最大数量。
- 每个 APN 的承载激活的最大速率。
- 一个 APN 的一个或多个分组数据网络 GW 是不可到达的，或者已经为 MME 表示拥塞。

基于 APN 的会话管理拥塞控制包含有来自移动设备的拒绝会话管理请求，例如，建立一个新的数据连接的请求，具有一个会话管理回退计时器。只要回退计时器正在运行，除了释放该连接，不允许移动设备为拥塞的 APN 启动任何会话管理程序。移动设备可能仍然会启动其他 APN 的会话管理程序。也允许移动设备启动优先级或紧急服务或响应寻呼的会话管理程序。移动设备将为移动设备可能激活的每个 APN 保持一个单独的会话管理回退计时器。

一个 MME/SGSN 可以检测与一个特定 APN 相关的移动性管理拥塞，并且通过监视与一个特定 APN 相关的移动性管理信令请求的最大速率，开始和停止执行基于 APN 的移动性管理拥塞控制。基于 APN 的移动性管理拥塞控制包含拒绝由移动设备启动的连接请求，移动设备具有一个特定的与一个移动性管理回退计时器订阅的 APN。直到计时器到期，除了优先级或紧急服务，不允许设备启动任何移动性管理程序。

6.3.7.6 防止来自网络重选的过载优化

为了保护一个被接入过的网络免受由这个国家中的一个（或多个）其他网络的故障造成的任何过载，已经定义了下面的机制。

移动设备可以由制造后配置得到配置：

● 对于更多的首选网络，具有一个较长最小周期的网络搜索时间限制在它们的搜索之间有一个增加的最小时间。

下面的一个首选网络的故障，移动设备可能会改变其他本地竞争网络。搜索计时器的到期会导致移动设备重新尝试接入首选的网络，然后，如果该网络尚未恢复，重新接入本地竞争网络中的一个。使用定期网络搜索的一个过短计时器可能阻止故障网络恢复，并且在竞争网络上施加更多的负载。

● 为了在网络的更改上执行具有 IMSI 的一个附加程序，而不是做一个跟踪区域更新程序。

一般一个跟踪区域更新程序比一个附加程序更有效。但在一个网络更改的时间中，一个跟踪区域更新一般是不可以接受的，使用 IMSI 造成一个订阅的附加程序。避免跟踪区域更新程序会降低承载在本地竞争网络上的信息过程，因此使得该网络更可能存在其他网络的故障。

对一个 MME、SGSN 和 MSC/VLR 而言，可能的是信号较长周期的跟踪区域更新，路由区域更新和到移动设备的位置更新，以及为了预见订阅数据中的这些周期性计时器的移动运营商的选项。使用这些特定的订阅计时器，以及使用由移动设备标记的低接入优先级指示，MME、SGSN 和 MSC/VLR 可能分配较长的周期更新计时器到 M2M 设备。降低速率是可能的，其中的一个 UE 检测网络故障，从而减慢从一个故障网络到其他的本地竞争网络的设备移动速率。使用较长周期的计时器也使由 M2M 设备产生的信令负载降低成为可能。

6.3.7.7 扩展的接入限制

EAB 是一种机制，允许运营商控制来自特定的 M2M 设备的始发移动接入尝试，以便防止接入网络和/或核心网络的过载。为了依附到 EAB 指示，移动设备应该从属于被分配的 EAB。在拥塞情况中，运营商可以限制来自为 EAB 配置的移动设备的接入，同时允许来自其他设备的接入。对于接入限制，为 EAB 配置的移动设备被认为比其他设备更宽容。当一个运营商决定应用 EAB 是合适的时，在一个特定的区域中，网络广播必要的信息。

EAB 可能还有助于防止来自网络重选的过载。EAB 信息可能表明限制只适用于漫游移动设备，或只适用于不在它们首选网络上的移动设备。

6.3.7.8 拥塞和过载控制机制的评估

没有一个万全的过载机制适用于各种各样的过载方案。移动运营商将必须采用一系列过载控制机制，以保护他们的网络。表 6-6 表明了过载机制，这些机制可能在过载方案的一些例子中被激活。

表 6-6　不同过载方案中激活的过载机制

过载方案	过载控制机制
外部事件触发大量的 M2M 设备立即进行所有的附加/连接	低接入优先级配置的移动设备的网络过载控制
M2M 应用和/或 M2M 服务中的故障	基于 APN 的拥塞控制把故障应用作为目标
一个网络服务许多漫游 M2M 设备故障	扩展接入限制，长期最小周期网络搜索时间限制，在网络更改处与 IMSI 连接，长期周期的 TAU/RAU/LAU 更新计时器，一般核心网络移动性管理拥塞控制
新年前夜的一小时高峰	在这些周期期间，移动设备的网络过载控制可以拒绝 M2M 低接入优先级业务，低接入优先级配置的移动设备由无线接入或核心网络触发

参考文献

[22.011] 3GPP TS 22.011. Service Accessibility.
[22.888] 3GPP TR 22.888. Study on Enhancements for Machine-Type Communications.
[22.988] 3GPP TR 22.889. Study on Alternatives to E.164 for Machine-Type Communications.
[22.368] 3GPP TS 22.368. Service Requirements for Machine-Type Communications (MTC); Stage 1 (2011).
[23.888] 3GPP TR 23.888. System Improvements for Machine-Type Communications (MTC).
[23.682] 3GPP TS 23.682. Architecture Enhancements to facilitate communications with Packet Data Networks and Applications (2011).
[23.060] 3GPP TS 23.060. GPRS Service Description; Stage 2 (first published 2000).
[23.401] 3GGP TS 23.401. GPRS Enhancements for E-UTRAN Access (2008).
[OMA DM] Open Mobile Alliance Device Management Architecture (2006).
[TR-069] Broadband Forum TR-069 (2004). CPE WAN Management Protocol.
[33.220] 3GPP TS 33.220. Generic Authentication Architecture; Generic Bootstrapping Architecture (GBA) (first published 2004).
[ECC 153] Electronic Communications Committee (2010), Numbering and Addressing in M2M Communications, ECC Report 153.
[E.164] ITU-T Recommendation E.164. The International Public Telecommunication Numbering Plan (2010).
[E.118] ITU-T Recommendation E.118. The International Telecommunication Charge Card (2006).
[23.040] 3GPP TS 23.040. Technical Realization of the Short Message Service (SMS) (first published 1999).
[23.041] 3GPP TS 23.041. Technical Realization of Cell Broadcast Service (CBS) (first published 1999).
[23.002] 3GPP TS 23.002, Network architecture http://www.3gpp.org/ftp/Specs/html-info/23002.
[23.003] 3GPP TS 23.003, Numbering, addressing and identification.

第 7 章　IP 在 M2M 中的作用

Laurent Toutain，Ana Minaburo
布列塔尼国立高等电信学校，Cesson Sevigne Cedex，法国

7.1　引言

计算机网络协议的持续时间很少能跟 IPv4 协议的持续时间相媲美。即使一开始，IP 从未被设计成为通用的协议，我们知道，现在它已经发展成为足够灵活的，并能覆盖不断增加的若干应用。乍一看，此成功只与梅特卡夫（Metcalfe）定律的阐述相关联，该定律指出网络的价值（即用户可以从技术方面获得的效益）是用户数量的二次方。虽然参考文献［1］对公式 $n\log(n)$（其中 n 是用户的数量）进行了调和，但将导致良性循环的减弱：一方面，网络变得更具吸引力，而另一方面，对新协议或新形式行为的抵抗也增加了。

对普通大众来说，互联网是网络提供服务的代名词，但对网络工程师来说，互联网可以看成是由 IETF 的 RFC 791[2]在第 3 层定义的协议栈，一些传输协议，如 TCP[3]、UDP[4]，以及最近的 SCTP[5]或 DCCP[6]和最终的一些应用，例如 DNS[7]。

网络的另一个定义是基于其本身的实际名称，因为它是由互连和网络构成的，有时使用“网络的网络”来代替。这个更普遍的定义并没有考虑到一个事实，即任何一个协议会导致更多的“哲学的”方式，这在网络设计和架构中变得比协议本身更加重要。这是对 M2M 通信更加精确的定义。当前的互联网协议开发不适宜 M2M 的约束条件。不考虑能源约束。互联网协议有时是非常复杂的，或需要在可升级的环境中陈述出那些不具备的条件。定期服务或引导程序的自动配置是必要的，因为这些项目的设备并不一定有键盘或设备的大规模资源配置，也不允许手动或管理配置。支持 M2M 和无线传感器网络（WSN）的互联网进化，需要的不仅仅是在路由协议里的几个简单的变化。协议、路由算法和对地址有修订作用的应用设计，这些都会导致报头格式的大幅重新定义。另一方面，具有互操作性的现有设备和当前的应用是必要的，否则，对包括互联网协议在内所做的所有努力都将是徒劳的。

互联网正在进行激烈的协议进化。数据包格式改变为 128 位的地址，而不是最初使用的 IP 的版本4（IPv4）的 32 位地址。目前预测在 2012 年，IPv4 的地址空间将被用尽。新版本的互联网标准（IPv6）已标准化，但即使一些主要参与者在他们

的网络设备中已经囊括了 IPv6，IPv6 的实际资源配置仍然非常有限。梅特卡夫定律与 IPv6 相背离，因为大多数的服务或内容只适用于 IPv6，而在使用新版本的协议时没有真正的需求。由于没有迫切的需求，部署新的应用或许有更大的难度，协议版本 4 和版本 6 的需求仍然很低。IETF 已经预见了这种情况：同时运行两个版本的协议已经不可行了，最可能出现的情况是供应商将会在核心网络采用 IPv6 的地址，在其余的传统应用中能使用 IPv4。

如果 IPv4 仍然为传统应用的主协议，在新的电信领域内将造成大规模的资源配置不能被 IP 版本所支持。如果不考虑路由协议的约束条件和分配政策，32 位的 IPv4 地址理论上只允许容纳 40 亿件设备。如果考虑可以与互联网相连接的汽车、机器和传感器的数量，这个数目是比较少的。在未来的服务中，IPv6 的出现是一个具有吸引力的解决方案。某些新的网络基础设施，如 LTE，也选择授权 IPv6。

7.1.1　IPv6 简介

IPv6 协议是 IPv4 数据包的一种简化，并保留了相同的规则。经过多年开发，无用的字段已经被移除。使用一系列固定格式的扩展头部取代了 IPv4 中可变长度的选项字段。扩展可以看成是第 3 层（IP）和第 4 层（UDP，TCP）之间的媒介协议，除了逐跳扩展必须由路径上的每个路由处理，其他扩展从核心网络是不可见的，只由最终的目的端口处理。如今，很少有扩展真正用于分离 IPsec 的定义。它们主要用于管理移动 IP 的移动性和多宿主 shim6。

存储碎片已从主标题信息中移除，现在将其看作是一个扩展。这将产生一个有更高稳定性和可预测字段的更简单的数据包。尽管 IPv6 地址的大小是 IPv4 地址的 4 倍，但报头的大小仅仅是一个 IPv4 报头的 2 倍，如图 7-1 所示。

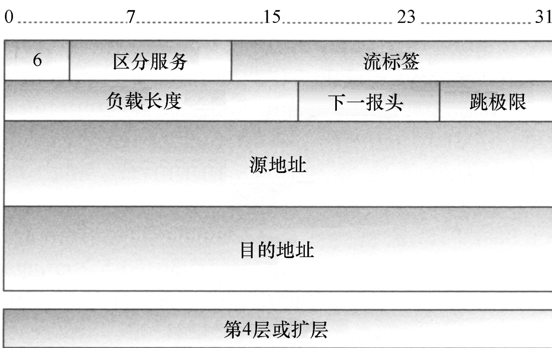


图 7-1　IPv6 报头结构

IPv6 引入的唯一的新字段是流标签，在早期的 IPv6 设计中，流标签曾尝试在

核心网络允许简单的流动识别，由于使用扩展，所以第 4 层端口号不能像在 IPv4 中一样容易进入。随着多协议标签交换（MPLS）重新定义了流的概念，流标签的使用开始变得不那么重要了。

两个版本的 IP 协议之间数据包格式的修改创建连接，使用应用层网关（ALG）或复杂的报头译文来保证 IPv4 和 IPv6 应用之间的兼容性，但网络管理方式保持不变。地址分配和路由选择仍然遵循 CIDR 规则。与 IP 发展相关的大多数协议要考虑更大的地址，而不改变其算法。

IPv6 所提供的大地址空间不仅允许更大数量的设备可以与互联网相连接，而且简化了网络管理的约束条件。比 IPv4 更清楚，IPv6 的地址分为三部分，如图 7-2 所示。第一部分，全局前缀（GP），由 ISP 分配，用于在互联网核心的 IPv6 数据包路由。站点网络管理员分配第二部分是子网络标识符（SID），它把内部的数据包转发到相应网络。GP 和 SID 必须填满地址的前 64 位。一般来说，GP 的长度是 48 位，SID 的长度是 16 位，但是站点的大小和供应商不同，其长度也是不一样的。剩下的 64 位地址专门用于接口识别（IID）。以十六进制的 16 位字表示地址符号，并用“:”相隔。一个冒号重复两次代表一个单独的长零序列，但这在一个地址中只能使用一次。

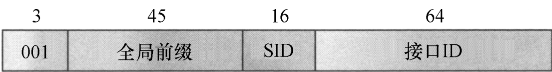


图 7-2 IPv6 报头结构

分配 IID 有几种不同的方法。起初，IID 来自接口的 MAC 地址（MAC-48 或 EUI-64），这种确保单一分配的链接的简单方式有一定的缺陷：即使设备从一个网络移动到另一个网络，并改变了 GP：IID：：/64 部分，它的 IID 保持不变，有些服务器却可能随着设备而变化。MAC 地址内含有一个表明电脑品牌的组织唯一标识符（OUI），有些公司可能不愿意把他们网络之外的信息传播出去。为了打消这种顾虑，可以随机抽取 IID；较大尺寸的 IID 和相对较少数量的设备相连接使所发生的冲突大大减少。

无论是随机或者是基于 MAC 地址，由于 IID 不可预知，并且对一个网络管理员来说它不容易记住，所以非常难管理。可以给 IID 手动分配一个容易记忆的较小的值，也可以从证书（密码生成地址，CGA）中获取 IID，这种方式的 IID，主机在网络中已被认证。

IPv6 定义了其他前缀：

- FE80：：/64 与随机 IID 生成或 MAC IID 生成同时使用，用于创建本地链路（LL）地址。使用这些地址的数据包不能使用链路之外的路由，但其用于引导程序期间时，允许起始主机在第 3 层用一个称为“邻居发现”的协议创建配置（见

第7.3.3节)。LL地址也能在路由表中找到。

● ULA（unique local address，唯一本地地址）是由站点生成的随机前缀构成的。携带这些地址的数据包不能离开站点，但在该站点没有连接IPv6或全局互联网隔离某些设备的情况下可以使用，这也是IPv4有私有地址的原因。

● 多播前缀从FF00::/8开始。前缀的后四个比特包含一些用于管理大型多播网络的标志，接下来的四个比特位给出多播的范围（1表示多播仅限于主机内部的通信，2用于链路通信，5限制一个管理实体等)。

● 一些特殊的定义：例如，FF02::1用于给与发送者链路相连接的所有设备发送数据包，FF02::2代表与发送者链路相连接的该组路由器。

7.1.2　邻居发现协议

邻居发现协议（NDP）是自动插入主机进入IP网络的一种新方法。对于IPv4，使用DHCP客户端/服务器的方法是一种可行的办法，尽管DHCPv6也可以用于给主机分配地址或给路由器分配前缀，IPv6重新定义了DHCP，但主要用于分配静态参数，如DNS服务器。IPv6推广无状态自动地址配置（SLAAC）机制。NDP使用四个特殊的ICMPv6消息——RS：路由请求；RA：路由广告；NS：邻居请求；NA：邻居公告。第一对消息用于一个节点和一个路由器之间的交换，后一对用于两个节点之间，主要通过IPv4中的ARP来解决IPv6地址和MAC地址之间的映射。

当一个节点初始化时，它会使用熟知的FE80::/64前缀创建LL地址并连接它的IID，在测试之前，没有任何其他主机用这个地址发送NS请求映射自己的LL地址，如果没有响应，节点可以假定LL地址的唯一性，并且可以使用它与路由器进行通信。这个阶段被称为DAD（地址重复检测)，并可以发送几个NS探针以确保在链路上既没有请求也没有应答已被丢弃。

如果DAD成功，该节点可以使用RS消息查询路由器的配置参数，路由器应答中用到几个参数，例如：

● 链路使用的前缀和其长度。

● 节点是否可以通过把接收到的前缀与它的IID相连接来构造全局地址，否则，必须发送一个DHCPv6请求以获得全局地址。

● 一些静态参数是否可以通过DHCPv6获取。

● 链路是否是一个节点可以进行相互通话的广播链路，或是一个所有通信都必须通过路由器的非广播多址（NBMA）链路，如果这样的话，因为路由器知道这种映射，所以不需要地址解析（NS/NA交换)。

● 链路使用最大传输单元（MTU）和跳数限制（HL)。

在RA消息中配置包含前缀的地址的节点将使用应答路由作为默认路由，GP的唯一性也用DAD来检测，为了避免必须使用DHCPv6查询来获得DNS解析，RA

消息也可以选择包含解析器的 IPv6 地址。

7.2 M2M 中的 IPv6

在 M2M 网络中，并不是所有的设备都具有相同的运行网络的功能，这最初是为 IPv6 定义的，不考虑能源和频带消耗，假设 IPv6 传输支持具有接近以太网的功能。无线传感器网络（WSN）是已表明这些制约因素不太现实的第一个领域，它们仅包括 M2M 网络（包括 3G 网络）中的一部分，却是新网络领域的代表。就在不久前，对 WSN 的应用直接设计了一个二层协议，如 IEEE 802.15.4，灵活性有限，因为整个网络部分，如路由，必须为每一种情形所完善。这将使不能直接与互联网的其他设备对话的程序中断，ZigBee 论坛定义了协议栈和传感器的配置文件，还有具有更好的互操作性的驱动器，网络也可采用不同的方式携带警报系统信息和照明控制。不过，ZigBee 网络是一个“有围墙的花园”，通过应用网关与外界进行通信，这将使新服务的部署更加复杂，因为必须要考虑采用新程序对网关进行改良。

如前面所述，由于路由器不考虑应用，能从一个接口把数据包转送到另一个接口，并能使数据传送与媒体性质的反映相适，即 IP 提供了一个更加灵活的体系结构。在 IETF 的 6LoWPAN 工作组从事于允许 IPv6 在 LoWPAN 转发的适配层，即使 LoWPAN 网络的定义比 IEEE 802.15.4 更广泛，但其工作的重点主要是针对低功率的环境。

如果一些家庭自动化应用，可以支持 ZigBee 封闭模式，如灯光控制，另一些，如 ZigBee 智能能源需求与外界的互连，有些信息必须与能源提供者进行交流，以在能源价格上采取措施，所以全局互连是必要的。ZigBee 论坛已为属性选择了 IPv6。在其他领域，也做出了相似的抉择，在行业内的 ISA 定义了传感器标准，他们同样选择了 IPv6，但不是因为它的互连功能，因为工业生产过程主要是本地控制，但为了得益于成本降低产生的配置设备已开发成为大众市场。

关于 IPv6 和 LoWPAN 网络相关的主要制约因素有以下几点：

● 在 IPv6 定义的标准[8]中，链路层必须支持带有最低为 1280 字节的有效负载的数据报文，此限制源于 NDP。NDP 消息，尤其是 RA，不该被分割，该值也可以允许一些封装的 IP 报头支持隧道，该标准还规定，如果一个链路层不能支持该最小值，适配层必须隐藏这些制约因素。这是 ATM 和适配层 AAL5 的一个示例。

● 对 WSN 来说，已开发了一种新的适配层，用于支持 IPv6 报头压缩和更精确的支持允许广播和路由设施的第二层协议。

● 如前面的章节所述，IPv6 使 NDP 协议适应于 WSN，在链路中以产生干扰多播通信。此外，在 LoWPAN 中，链路没有得到很好的定义，因为框架范围随着时

间的变化非常快，这种适应将由大大减少的信息数量构成，这些信息是由协议和一些熟知并可达成的项目的设备产生的集中信息。

研究路由超低功耗和有损网络（Roll）的 IETF 工作小组目前正在开发一种路由协议，这种路由协议的性质由底层链路和通信模式构成。他们正在研究 WSN 的 RPL 协议，RPL 考虑到节点之间的联系随着时间的推移发生变化，主要归因于无线电信号的弱点。最后，第四层协议，如 TCP 用于控制，并不总是适合于与传感器之间的通信。面向连接协议的开始和结束阶段对简单的查询/响应交换来说太繁重了，TCP 也是一个非常复杂的协议，在传感器内存里需要大量覆盖区有效地处理连接问题，一些简单的查询/响应方案可以部署在 UDP。IETF CoRE 工作小组目前的重点是关于这一主题的研究。

7.3　6LoWPAN

6LoWPAN 工作组旨在使 LoWPAN 网络可以支持 IPv6 协议，其主要目标是确保互联网和 WSN 之间的互连，以使 IPv6 协议和如 NDP 的相关协议适用于 6LoWPAN 的网络特性。在传感器节点和一个或几个 LoWPAN 边界路由（LBS）连接到公共网络时使用 6LoWPAN 协议。LBR 设备包含路由器的功能，也可以压缩、解压数据包。IPv6 适于 LoWPAN 环境需要一些约束条件：

● 与以 1280 字节的最小值命令 MTU 的 IPv6 规范相比，第二层帧的大小可能会受到限制。提供由 IPv6 RFC 指定的帧长度时采用分裂的方法。

● 在某些节点上，能量严重受限，例如，相同的电池上一些计量装置运行几年（最多 15 年），必须避免不必要的交换和多播流量以节约功率。

● 不能将邻居发现消息分段。如果丢失了某些片段，协议的效率将大大降低。

● 无线电射程可能会减小，IPv6 数据包必须从一个节点到另一个节点进行转发，以到达目的地或一个 LBR。

● 在有线网络或 WiFi 网络中，邻域没有被很好的定义，无线电射程变化导致邻居列表发生改变。

一个 6LoWPAN 网络可以由三种拓扑结构构成：

● 星形拓扑结构：所有的传感器节点都可以到达，并可以从 LBR 获得。

● 网状：为了向目的地转送帧，在第二层组织节点，形成互连的算法没有被 6LoWPAN 定义，它只是提供了通用的支持来管理广播和逐跳桥接。从互联网的视角看，与以太网网络类似的网状网络每个节点共享相同的前缀，6LoWPAN 把这种技术作称作 mesh-under（MU）。

● 路由：节点充当路由器用来向目的地转发数据包，必须在某些节点上运行路由协议以构建转发信息。节点在 LoWPAN 网络内部充当路由器，而不是直接与

互联网相连接，这种节点称为 LoWPAN 路由器（LR）。6LoWPAN 称这种技术为 route-over（RO），Roll 工作组定义的 RPL 协议是最佳的候选协议。

7.3.1 框架

有两方面的内容：第一方面，为了使开销最小，压缩的 IPv6 报头和上述的协议允许简单查询和 NDP 信息保持在一个单一的有限容量的帧；第二方面讲的是使 NDP 适应链路的特殊性，尤其是当 NDP 必须与路由协议相互作用的情况下。

7.3.2 头信息压缩

6LoWPAN 没有链接到特殊形式的技术，然而，目前的实现主要是基于 IEEE 802.15.4。MAC 协议网络定义了四字节的帧：信标、数据、确认和控制，如图 7-3 所示。每一个以 32 位的前导码和一个起始帧分隔符开始的同步接收机。接着是七位的允许最多为 127 字节的数据长度编码，此后，帧控制字段给出了一些信息，如帧的类型，存在源地址和目的地址（16 位 64 位）的大小，使用 PAN（私人局域网）标识（PANid）。用于识别和应答帧的序列号，当帧转发由 PANid 组成的地址字段和目的地址与源地址时，不需要确认，当其他部分包含数据时，仅确认帧是空的，所有的四个类型的帧均以 CRC 结束。

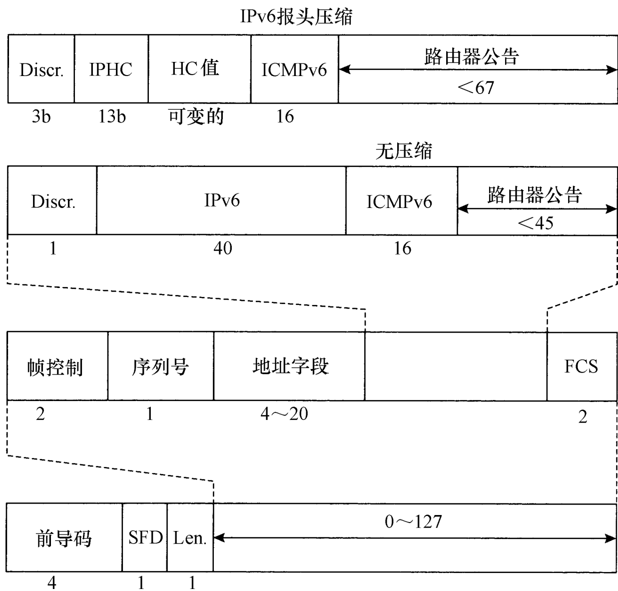


图 7-3 IEEE 802.15.4 RA 封装

该协议允许最大数据为 127 字节，但是 IPv6 标准规定 1280 字节为最小值。6LoWPAN[9] 含有一个适应这种约束的碎片协议，6LoWPAN 还提供了一种减小 IPv6

报头尺寸的报头压缩机制，从而避免了发送众所周知的信息或传感器网络层的信息发现。在标准中定义的压缩技术将很快被淘汰，而以称为 IP 报头压缩（IPHC）的更有效的版本替代[⊖]。在这种情况下，我们只介绍这种新的报头压缩算法。该协议还转发某些用于网状网络或广播支持的字段，但也有没定义的协议，因为第二层协议超出了 IETF 规范的范围。6LoWPAN 也可能会定义 L4 报头压缩。目前，UDP 只存在一种机制，但是对其他协议，如 ICMPv6 或 TCP，也应该尽快覆盖。

6LoWPAN 定义数据字段的第一个字节用于识别，该识别表明数据是如何构造的，例如：

- 01000001 表示保留位包含一个未压缩的 IPv6 报头。
- 011 表示使用新压缩方案将报头压缩。
- 10 表示一个网状封装就是源地址和目的地址。
- 01010000 在网状拓扑结构里转发一个标签限制广播帧的传播。
- 11000xxx 和 11100xxx 表示一个分裂报头就是各自的初始碎片和剩余碎片。

在帧中设置一些固定的值，采用这种方式简化解码，如果采用此种方式，帧必须以网状报头和广播报头为开始，接着是分裂报头，最后是 L3 报头（压缩或不压缩）和 L4 报头（压缩或不压缩）。

即使为了避免与 ZigBee 数据帧发生冲突而选择识别值，仍没有可靠的方法来区别 6LoWPAN 数据包和 ZigBee 数据包，所以这些协议中仅有一个协议在任何给定的时刻运行于 WSN 中。

图 7-3 给出了一个 ICMPv6 信息带或不带 IPHC 压缩的例子，在最好的状况下，与 40 字节的初始报头相比，IPHC 识别能减少到两字节，然后转发值。对于更多压缩结果细节，参见 7.3.2.5 节。接下来讲述识别行为。

7.3.2.1　ID 接口

6LoWPAN 受益于来源于 MAC 地址的 IID，因为期望 MAC 地址的唯一性，DAD 算法将不需要保证 IPv6 地址是唯一的，这也将帮助 6LoWPAN 改进压缩程序。如果在第二层转发地址，就不需要把它再送到第三层。

若第二层地址以 16 位编码，在 IID 前面将连接 0000：00ff：fe00。

7.3.2.2　网状识别

在无线网络里，位于无线范围里的每个节点都能接收帧，如果所有的接收者向目的地复制帧，目的地将收到初始消息的一些副本。为了避免这种情况，发送者必须指定哪个节点将向目的地转发帧。在网状网络中，帧头里的地址用于设计逐跳节点，即真正发送帧的节点是它的邻居，邻居向目的地转发帧。网状报头如图 7-4 所

⊖ RFC 6282。

示，4 转发端到端地址。V 和 F 位用于表明源地址（第一地址）长度和终端目的地；如果设为 0，长度是四字节，如果设为 1，长度是 16 字节。识别完成后给出地址值。左跳字段用于限制网状网络中无线循环的影响。



图 7-4　网状识别

6LoWPAN 没有为发现下一跳地址作为特定目的地而定义任何特定的算法。用于 MU 转发的识别用途并不是十分的广泛，而更偏好 RO，用每个节点充当路由器。在这种情况下，不再需要识别。当路由表给出下一跳时，数据包依照目的地址被转发。路由协议，如 RPL，用于填满路由表。

7.3.2.3　广播识别

如果一个广播帧需要到达 WSN 中的所有节点，或实现简单但无效的多播，那么必须执行一种泛滥机制。广播识别转发信息以避免循环。八位识别后，源选择一个八位的唯一序列值。即使 RFC 不指定使用方式，这种算法也相对较为简单。当使用广播识别转发信息时，在一段时间内，节点会保存源地址和这个序列值。如果在这个间隙内，新的帧收到相同的源地址和序列号，那么这个帧将被抛弃。

7.3.2.4　分裂识别

如图 7-5 所示，有两种识别控制分裂。其识别程序与 IP 使用的非常相似，路由器选择一个标签执行分裂，用来区分属于不同的数据报文的碎片。

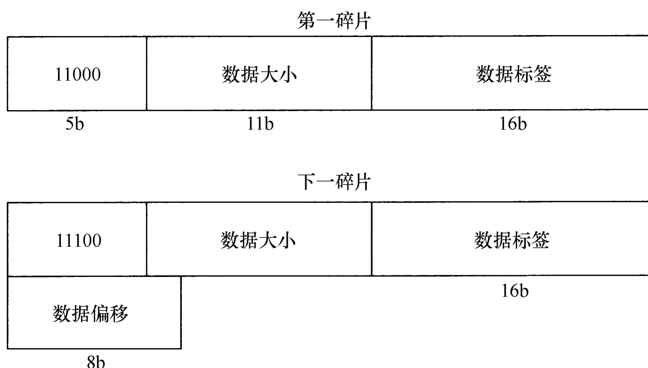


图 7-5　分裂识别

除转发初始数据中的偏移位置，所有碎片转发初始数据报文长度和所有的碎片。

7.3.2.5　报头压缩识别

IPv6 报头压缩是 6LoWPAN 协议中最重要的一部分，这种压缩是无状态的，即意味着没有 Context 信息保持压缩或重建数据报头。用这种方法，可以发生重编路由，数据报文可能通过不同的 LBR 丢弃。这种压缩方案是基于这样一个事实，即 IPv6 报头的大部分字段是不可预知的，所以可以测量其长度；流标签常设置为 0，如果包括 EUI-16 或 EUI-64 的 IPv6 地址建立，此值将不需要发送，因为它可以在第二层帧里被发现。前缀部分压缩时要更加复杂，由于在参考文献［9］中对于链路层地址压缩仅是最理想的，并仅对 NDP 有效。RFC 6282 把压缩机制推广到任何种类前缀和多播地址，由于前缀是不可预知的，故能存储在一些表中，压缩机制为了适用于特定前缀将使用指针。

数据包以 3 位识别码开始，接着是 13 位位图描述，即必须发送部分初始 IPv6 报头，其余部分可以不用发送。图 7-6 给出了不同标志的值。

011	TF	NH	HLIM	CID	SAC	SAM	M	DAC	DAM
3b	2b	1b	2b	1b	1b	2b	1b	1b	2b

图 7-6　IPHC 识别

当标志的所有位被设置为 0 时，与编码协定一致识别后在线发送该字段。如果设置成 1，省略该字段。因为所有字段的长度已知，目的地很容易恢复其值。

TF（业务类别，流标签）覆盖 DiffServ Field（DSCP：六位）、拥塞指示（ECN：两位）和流标签（20 位）。标志值既避开了 DSCP 又避开了流标签。

下一个报头（NH）标志指定如何处理第四层协议，如果标志被设置为 0，向 IPv6 报头发送未更改的 NH 字段，如果设置成为 1，另一个标签表示上面的压缩机制在 IPHC 报头之后可以被定义。目前，该标准定义了两种可能标签：一种是对 IPv6，它能用于 IPv6 的扩展或 IPv6 通道，对 UDP 也是一种简单的压缩方案。另一种机制在将来对第四层协议可能会被定义，例如 TCP。

HLIM（跳数限制）标志定义了一些除在线值之外的已知值。

Context 指定一个前缀都可以被每个传感器识别，使在每个 IPHC 报头中不再发送前缀值。一个单一的 Context（0x）是在默认情况下被定义的，该 Context 不同于源地址和目的地址。当 CID 标志被设置为 1 时，表明可以使用 16 Context。在这种情况下，识别后就增加了额外字节的信息。Context 字段的前四位指定源前缀值并保留四位作目的前缀值。Context 序号和值之间的同步可通过对 WSN 增加 NDP 来实现（参见 7.3.3 节）。

SAC（源地址压缩）标志为源地址给出了前缀的特性，如果标志设置为 0，该前缀大部分为 LL 前缀，表 7-1 给出了可能值。

表 7-1　SAC 和 SAM 位

SAC/SAM	00	01	10	11
IID		前缀的前 64 位未发送，IID 全部发送	前缀的 112 位未发送，最后 16 位 IID 发送	128 位未发送
0	完全发送地址（本地连接和全局）	前缀为 FE80∷/64	前缀为 FE80∷0：ff：fe 00/112	前缀为：FE80∷/64，从 L2 源地址获取 IID
1	未指定的地址（∷/0（not sent））	前缀由 Context 给定	前缀由 Context 给定，IID 以 0000：00ff：fe00：和 16 位联机开始	前缀由 Context 给定，从 L2 源地址获取 IID

压缩根据拓扑结构而不同，SAC/SAM（源地址模式）=0/00，由于它没有形成任何压缩，所以在任何情况中都可以使用。SAM =11 主要是为星形拓扑和 MU 网络所定义的，因为 L2 地址必须在报头出现，如在 IEEE 802.15.4 报头或网状报头分别存在。由于逐跳转发要求包含 L2 报头的信息须严格局限于两跳之间，故 SAM =01 或 SAM =10 可以用于 RO 拓扑，如果这两个值是 64 位或 16 位，那么它们对于区分地址编码之间的长度是必需的。

对目的地址来说，该规则仍保持不变，一个发现地址确认（DAC）标志表明前缀是本地连接还是从 Context 连接。目的地址同样能用作多播地址，所以增加一个 M 标志用来区别单一地址。表 7-2 给出了可能值。

表 7-2　M、DAC 和 DAM 位

M-SAC/SAM	00	01	10	11
00	完全发送地址（本地连接和全局）	前缀为 FE80∷/64	前缀为 FE80∷0：ff：fe 00/112	前缀为 FE80∷/64，从 L2 源地址获取 IID
01	保留	前缀由 Context 给定	前缀由 Context 给定，IID 以 0000：00ff：fe00：和 16 位联机开始	前缀由 Context 给定，从 L2 源地址获取 IID
10	完全发送地址	联机发送 48 位并在多插地址，如 FFXX∷00XX：XXXX XXXX 中传播	联机发送 32 位并在多播地址，如 FFXX∷00XX：XXXX 中传播	联机发送 8 位并在多播地址，如 FF02∷00XX 中传播
11	发送48 位，用于如参考文献［11］中定义的大规模多播。Context 含有集合点地址	保留	保留	保留

7.3.3　邻居发现

在 LoWPAN 网络中，无线范围被限制，并不是所有的节点都可以直接进行对话，而且，无线范围可能会发生大幅的变化，例如，空气湿度水平或由其他网络或设备所引起的破坏等，这些都会影响无线范围。不能时刻保证双向通信，NDP 协议所依靠的连接定义，如参考文献［10］中所定义的，没有以太网或 WiFi 定义得清晰。NDP 必须能适应这些情况：不仅要考虑链路的特殊性，还要减少能源需求以保障节点与邻居对话的功能。

NDP 依赖第二层多播的扩展性能获得网络参数，由于以太网、WiFi 或网桥都支持这类通信，运行 DAD，或者移动节点以解决 IPv6 地址和 MAC 地址之间的映射问题。在 LoWPAN 中，多播意味着实现更加复杂：

● 在 MU 模型中，为了允许广播，定义了一个指定的调度值。一个 L13 多播地址可以容易地映射到 L2 广播地址中，但这将导致网络满溢，并且所有的节点都将必须处理该信息。

● 因 NBMA㊀网络的作用，RO 网络可以被接入，在 NBMA 网络中，指定的服务器执行多播。将 NDP 变为 RO LoWPAN，当一个节点需要发现邻居路由器时，将仅允许多播。一旦决定了路由器的地址，通信将使用单播。

● 此外，RO 网络主要由充当路由器的节点组成，来向目的地转发信息，但从寻址角度来看，它作为单一链路出现，相同的前缀可能被指派到所有节点。但 NDP 不同，通过构造，形成交叉路由器，因为规范最初打算使用物理链路。NDP 为 6LoWPAN 引进了多跳前缀的概念，NDP 不应该作为路由协议被接入，但允许物理可到达的邻居间的通信。在 LoWPAN 中的路由协议，如 RPL，所有属于一个 LoWPAN 的节点之间建立连接需要该协议。

另一种减少多播通信量的方式是避免周期的 RA 作为通知路由器的状态和 LoWPAN 前缀值的邻居节点的方法。LoWPAN 网络中，在地址结束前，必须核实每一个节点，前缀和网络参数仍然有效。

DAD 用法也进行充分的复审，DAD 基于一种用于确保还没有被指派到其他节点的暂停机制。在 LoWPAN 中，由于邻居节点临时不可到达，可能会超出暂停，这意味着 DAD 处理将无效。

在 LoWPAN 网络中，如果没有准确地遵守 IEEE 标准，在这种情况下，假定 EUI-64 是唯一指定的。从 IEU-64 中获得的 LL 地址是唯一的，但不需要为了保证唯一性去核实。通过 DHCPv6，同样的假设可以用于既定的地址，对其他地址，如

㊀ 非广播多路接入：任何节点都可以到达，但一次只有一个节点可以到达，就像电话网络一样。

随机值或证书产生的值，一些中心元将转发确认，这将维持用于其域的地址列表和发送的 MAC 地址。

以减少通信量和避免多播信息的使用为目的，当节点需要时，抑制周期的路由广告信息并仅使用单播发送 RA。

7.3.3.1　本地连接地址

LL 地址应该是在线状态，因为 IID 基于 MAC 地址并定义它们分享共同的媒介（也就是说，在源和目的地之间没有路由器）不需要地址解析。在 MU 模式中，LL 地址可用于到达位于 LoWPAN 的任何主机。第二层维持一类路由协议（IETF 没有指定）到达任何其他节点。在 RO 模式中，LL 地址仅用于直接联系采用无线接口可到达的邻居。

图 7-7 是邻居发现的一个例子。每个节点设计了一个唯一的第二层 EUI-64，邻居节点通过把 FE80∷/64 与各自的 EUI-64 值相连接建立 LL 地址。如果在第三层，节点 1 必须向节点 2 发送数据包，节点 2 的 MAC 地址可以从 IPv6 地址中提取。

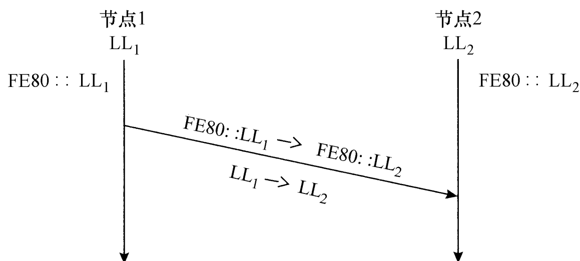


图 7-7　邻居发现

7.3.3.2　全局地址

与 LL 地址相反，全局地址没有办法在基于 IUE-64 的 IID 和随机值之间进行区分。由于这个原因，这类地址可用离线模式进行管理。IPv6 定义这种模式（携带 RA 信息）为命令将所有的数据包发送到默认路由第二层地址，这将使周围主机拥有更好的视域，并能解决该地址和 MAC 地址之间的映射问题㊀。要使路由器理解 IP 和 MAC 地址之间的映射，节点必须记录它们的地址。同时记录也为核实唯一的路径提供一种简单的机制。

在 RO 拓扑中，使用一个路由器和两个节点的方案，图 7-8 给出了全局地址 NDP 的概括。在之前的方案中，许多节点基于自己的 EUI-64 建立 LL 地址，在最简单的情况下，不使用中继，所有传感器节点就可以发送和接收来自 LBR 的信息。

㊀ 关闭链接模式可以让路由器发送 ICMPv6 重定向消息来通知发送者目的地的 MAC 地址。这提供了一个更直接的对剩余的数据包的传输方式。

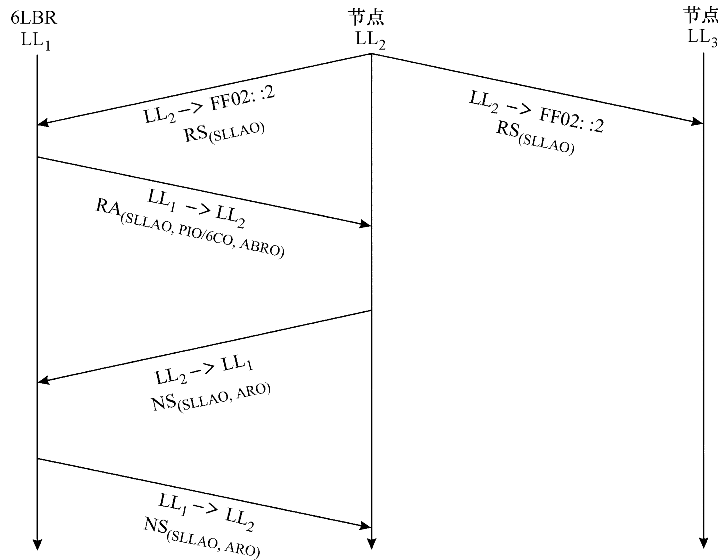


图 7-8　邻居发现

当一个节点进入网络时，需要经过以下这几个阶段。第一阶段是决定所有路由器并接收网络参数：

● 节点发送多播信息来决定邻居路由器，对于任何 RS（路由器请求），这个信息将给节点 MAC 地址一个选择权。

● 边界路由器（6LBR）和其他节点接收 RS，但只有 6LBR 路由器以包含 MAC 地址和前缀的路由广告（RA）应答，这个前缀是由 6LBR（PIO）和/或 6LoWPAN 的一个确定的选择来管理的，这种选择会映射一个 Context 标识符在 6LoWPAN 数据包中通知前缀（6CO）允许前缀压缩。未设置 L 位的值表示离线模式。

● 与 NDP 标准规范相比，最大前缀寿命可以设置为最大值（0xFFFF；大约 18h），边界路由器也可以增加一个将由其他 6LR 转发的指定选择项（ABRO：强制性边界路由器选择），利用这种方法，节点将知道边界路由器的 IPv6 地址，通知前缀并使用单播通信直接发送所有数据包。

第二阶段是记录全局地址：

● 为了检查地址的唯一性，发送含有 MAC 地址和临时 IPv6 地址（ARO：地址寄存选择）的单播 NS 信息，节点记录地址并委托给 6LBR。

如果节点已接收到了一些 RA 信息，该节点会把地址记录到所有 6LBR 中以增加可靠性。

● 邻居缓存路由器检查包含在 SLLAO 中的 MAC 地址和包含在 ARO 中的临时 IPv6 地址之间是否存在冲突。如果该入口是新的或已经存在，则不存在冲突，6LBR 以含有一个 ARO 的 NA 作应答，状态设置为 0。如果发现冲突（相同的 IPv6 地址，但 MAC 地

址不同)，状态返回为 1。如果邻居缓存已满，则返回状态 2。

若节点设置地址寿命为 0，路由器会从邻居缓存中移除该入口。

● 在冲突的情况下，节点可能选择其他地址（例如，通过产生一个随机数字)，并重新开始记录。

● 当节点 1 想向节点 2 发送数据包时，节点 1 给默认路由发送 IP 数据包，第二个节点以同样的方式严格地进行发现和记录地址。

● 路由器在邻居缓存检查目的地的 MAC 地址并向目的地发送数据包。

在 RO 模式中，节点不能直接到达 6LBR，信息必须由 6LR 进行中继。当接收到其他 6LBR 或 6LR 的 RA 时，6LR 进行信息副本的收集。当每一个都标记 6LR 的 IPv6 地址发布原始信息时，仅保持一个单一的原始通告。

在前面的例子中，一个节点发送多播 RS 信息，周围的 6LR 或 6LBR 以点到点 RA 信息应答，该节点使用一些路由器记录地址，遵循之前表述的流程。该时间是检查地址以防节点在相同路由器上记录的唯一可能的时刻。在整个 LoWPAN 上检查唯一性，路由器必须向 6LBR 发送请求指定前缀，这将通过两种新信息来实现，DAR（发现地址请求）和 DAC，它们分别用于打开主机发送的 NS 的通道和由 6LBR 给定的 NR 状态。

邻居缓存的路由器不是用于路由的目的；它仅允许链路联通性。在 RO 网状网络中，必须研发一种被其他路由器所知的路由协议来学习地址（或前缀，若有可能是聚类)。

7.4 低功耗有损网络路由协议（RPL)

在前面章节中介绍的 LoWPAN 网络能应用于不同的拓扑结构。星形拓扑是最简单的，但却不是最普遍的，因为 LoWPAN 必须覆盖比无线传输距离更大的区域，所以，在很多情况下，节点必须中继信息。如前面所示，6LoWPAN 体系架构包括两种方案：

● 第一，称为 mesh-under，假定定义一个 L2 中继策略，作用是使网状网络在 IP 层充当链路。

● 第二，称为 route-over，假定一些节点有路由能力并能向目的地转发数据包。

在本章中，我们将重点放 RO 体系结构上，它能更好地融合于 IP 体系架构。一些路由协议已经定义为固定的和 ad-hoc IP 网络。在一系列的 RFC[12-15] 中，Roll㊀工作组已经定义了不同网络架构的需求：

㊀ 该工作组与 6LoWPAN 工作组所做的工作是相互垂直的，因此他们所使用的词汇是不同的。LoWPAN 网络被称为低功耗、有损网络。设备也将有另外一个来自图论的名字，也就是说，6LBR 将被称为根，6LR 将是一个节点，如果 6LN 不能转发数据包，它则为叶。

- 城市网络。
- 工业网络。
- 家庭网络。
- 建筑网络。

现如今，现有的协议没有一个满足研究架构的特定需求。当连接着 ad-hoc 网络协议时，基于链路状态算法的协议（如开放最短路径优先（OSPF）或中间系统到中间系统（IS-IS））产生大量有效的通信，例如自组织网络按需距离矢量（AODV）或最佳链路状态路由（OLSR），可能使大量的传感器节点不能正确地衡量。

Roll 工作组定义的协议称为 RPL。它是基于距离的矢量算法，例如路由信息协议（RIP），是设计为改进由严重的循环探测引起的性能问题。在路由策略的定义中 RPL 必须也能保持灵活，一个城市网络不会和家庭网络一样拥有相同的约束条件，同样，在每一种网络类型里，应用不会总是共享同一个目标。可以试着用警报系统减少中继传播，而且应用产生定期的信息将设法用能量（Powered）的最高水平选择路由器。

图 7-9 显示了 Roll 工作组建立的不同规范之间的关系。RFC 标准[12-15]显示了不同应用情况下约束条件的多样性，RPL 将考虑路由协议使它的路由度量未知，基于秩概念，它表示了到根的距离。一些 RPL 的实例可能在单一节点上运行，每一个节点用于考虑不同的路由拓扑，RPL 信息包括不同的度量或约束条件更进一步地细化图表。目标函数定义了把度量变为秩的方法，目前，已定义了两个目标函数。第一个，OF0，是默认目标函数，当 RPL 信息不包含任何度量时使用该目标函数，路由选择是基于跳数的。第二个，最小秩滞后的目标函数（MRHOF），用于改变度量。即使由于很低的链路质量使度量迅速变化，之后仍用于维持路由选择的相对稳定。

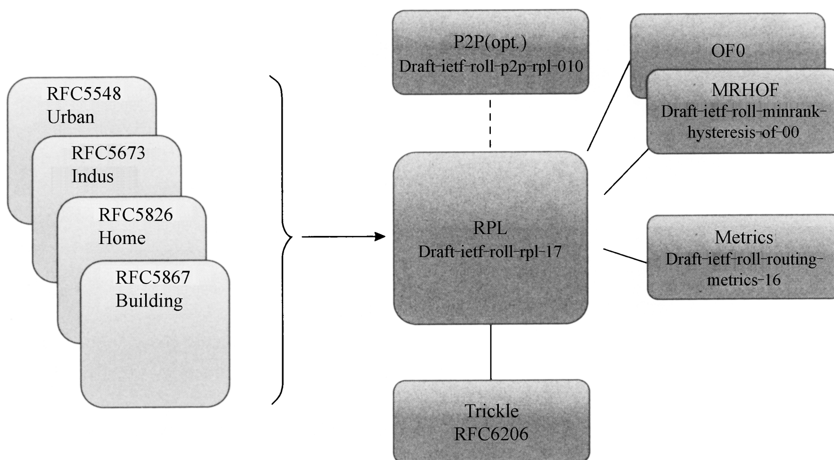


图 7-9　RPL 系

该工作小组的首要重点是处理上层通信：叶到根，也称作 MP2P（多点对点），下层通信：根到叶，称作 P2MP（点对多点）。当低功率有损网络（LLN）连接到传统互联网时产生 MP2P 通信，向/从 LLN 之外转发数据包。由于 M2M 在网关和多重设备之间是非常重要的，覆盖 MP2P 和 P2MP 是最重要的方面。这与 ZigBee Smart Energy 和 ETSI M2M 架构相符合。

P2P 通信（即是，位于相同 LLN 中的两个节点之间的通信）在第一个标准版本里不是最优的，向根发送 P2P 数据包直到到达能向目的地转发数据包的节点。另外一组草案[㊀]囊括了该优化。

为了减少网络发送信息的数量，一种 Trickle 算法可能限制发送周期信息的数量，在没有达到定义的最大值之前，节点定期发送相同信息将增加该周期。如果通告变化，周期被设置为定义的最小值，与 RIP 相比最重要的不同之处在于，缺少指示发送设备废弃的三个周期信息，Trickle 算法将延迟探测。节点必须展开其他策略去探测废弃的路由器，如邻居不可到达探测（NUD）或第二层确认。

7.4.1 RPL 网络拓扑

RPL 网络拓扑基于面向目的节点的有向无环图（DODAG），DODAG 允许上层通信离开 LLN，但后来也被用于为节点和叶建立相反的路径。与 RIP 相比的一个不同点为，维持目的地方向的单一路径，即 DODAG 可能包含更多目的地方向的无环路径，这将在路由故障的情况下增加可靠性并加速复原。

DOAG 架构依附于 RPL 协议规约定义的通用法则，同样遵循不同的目标函数文件中定义的更具体的行为模式（参见 7.4.1.2 节）。

一个单一的 DODAG 可以覆盖整个 LLN，但一些 DAG 可以组成一个 DODAG，同样，不同的根节点可用于 LLN，如图 7-10 所示，在这里，节点 11 和节点 51 是根节点。

节点可以运行 RPL 协议的不同实例，这将产生等效的 VLAN，并且每个实例可以用不同的度量和约束条件建立 DODAG。如果基于不同 DODAG 实例可以相对容易地建立不同的转发表，数据包将必须转发逐跳扩展以表明必须使用 DODAG 实例。

㊀ 草案-互联网工程任务组-卷-点对点技术-远程启动服务，草案-互联网工程任务组-卷-点对点技术-度量。

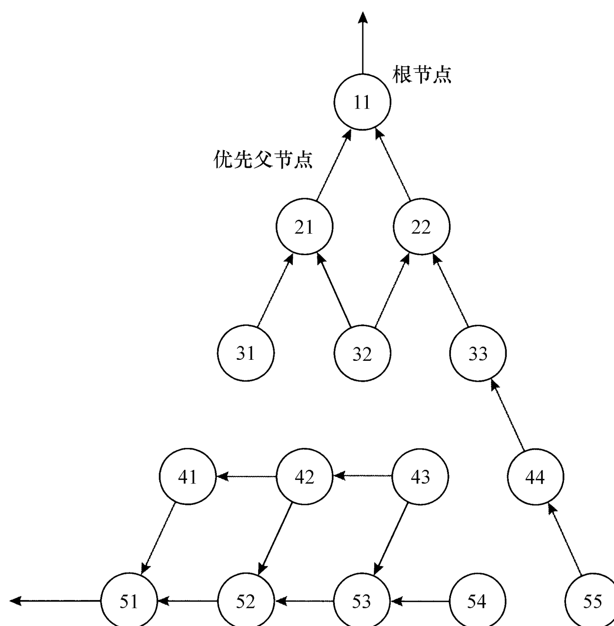


图 7-10　DODAG 与多个 DAG

根节点可以改变 DODAG 版本号，这是可以做到的，例如，在 DODAG 中发现了某些矛盾，这也许是由根节点信息遗失引起的，在这种情况下，新的 DODAG 被建立。

DODAG 可以接地，意味着 DAG 的根节点是一个边界路由器，在 DODAG 建立阶段或当与父节点失去连接时，subDAG 的根节点不可以作边界路由器，这时，DAG 应具有流动性。

7.4.1.1　邻居和父节点

除了叶节点，所有节点产生 DIO（DODAG 信息对象）ICMPv6 信息，该信息格式如图 7-11 所示，此图为了解 DODAG 的构造提供了可能。当证明网络稳定时，为了减少通信量，周期性发送 DIO 信息，周期由 Trickle 算法所决定。也可以发送 DIS（DODAG 信息请求）让其他节点响应 DIO，DIS 有限制应答邻居数量的权利。

节点使用从它的邻居接收的 DIO 信息决定它们的秩，并且，选择性地决定一些额外的度量和约束条件。根据信息和目标函数定义的规则，该节点选择上层通信发送的一组可能的父节点和优先的父节点，如果收到更好的秩通告，节点可以更容易地移动靠近根节点。

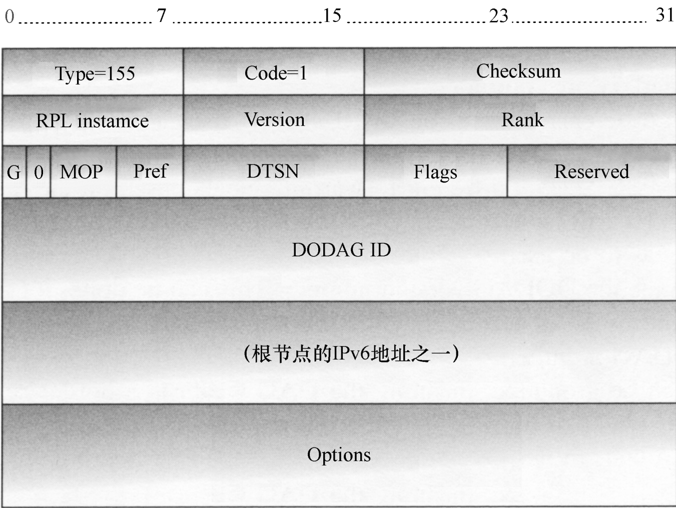


图 7-11 DIO 格式

如果一个节点必须增加它的等级，例如，当所有可能的父节点已经消失时，为了最小化路由循环的风险，运行会更加复杂。节点通过在 DIO 信息中设置 INFINITE_RANK 阻碍它的邻居，依次破坏 sub-DODAG 节点并且成为流动 DODAG 的根节点。如果秩没有增加，或自身成为流动的并仅重新附属于其他流动节点，节点接收该信息，但更喜欢依赖于其他的父节点。

相反，节点（或叶子）可以发送 DAO（DODAG 公告对象）通知一些地址（或前缀）父节点通过该节点可进行存取。通过转到根节点，该节点将填写路由表。然而，由于存储器的极限，一些节点没有维护路由表的可能性。RPL 实现两种形式的行为：

- 存储模式，所有的节点有足够的资源存储向下地址，以便数据包转发到下一跳。
- 无存储模式，仅有根节点与网络拓扑保持联系。节点向根节点发送 DAO 信息，其中包含它们的地址和父节点。根节点可以找到到达目的地的路径并且发送数据包，例如，IPv6 路由扩展包含必须交叉的路由器列表。

7.4.1.2 目标函数

目标函数适应网络路由到应用的行为，不同形式的行为是可能的，并能在不同的 RPL 实例中并行运行。根节点周期性洪泛代码点定义目标函数应用于 RPL 实例。

目前定义了两种目标函数：

- OF0：这是一种非常简单的行为形式，如果该节点既不实现由根节点通告的目标函数，也不实现包含 DIO 通告的度量容器，那么它可以用来作为最后的方法。

这将形成使跳数最小化的拓扑，例如 RPL，对于一个 LLN 来说，它不是最佳的路由选择。

- MRHOF：秩计算基于包含 DIO 信息的度量，这些度量比跳数更具动态性，可以考虑，如链路质量。MRHOF 仅用作附加的度量（如该值每增加一个节点交叉的时间）并避免造成不稳定的路由。只有当它明显不同于当前优选父节点路由时，一种迟滞机制允许选择一个更好的根节点。

7.4.1.3　度量和秩计算

RPL 打算使用不同度量和约束条件建立拓扑，度量的使用可附加（如路径质量）、可报告最小或最大值（如路径上节点的能量）并最终可倍增（如路径上的错误率）。额外的约束条件用于扩展 DODAG 的范围，选择使用的一个标准是独立于度量本身的，例如，链路质量可以被看作是一个附加度量或最小度量。度量和约束条件同样与节点相关：

- 能量：如何启动节点和剩余能量的百分比。
- 跳数：交叉主机数。
- 吞吐量，时延。
- 链路质量水平：从 1（最高）到 7（最低）。
- ETX（期望传输次数）：成功发送数据包的传输次数。

7.5　CoRE

前面的章节阐述了如何使设备之间或至少是设备与网关之间产生连接。CoAP（Constraint Application Protocol，约束应用协议）是基于表述性状态转移（REST）范例构造信息交换的一种方式，而 M2M 应用进行了优化。

HTTP 是 REST 架构中最典型的例子，一些简单的命令，如，GET 和 PUT，允许文件从服务器接入或送至服务器。REST 架构也能应用于传感器领域，GET 可用于接入值，PUT 存储值或触发激活。但对设备来说，HTTP 和 TCP 太过繁重，如传感器。优选 UDP 用于简单的查询，可简化的 HTTP 使数据消息的解析变得更容易，同时也能降低其开销。

CoAP 可以用于压缩简单的 HTTP 接口，而且还提供了内置的发现、多播支持和异步处理。CoAP 定义：

- 一个简单的报文格式由处理资源有限的设备轻松地处理。
- 一个简单的传输协议检测和纠正数据包丢失。
- 在节点使用 REST 范例查询或存储信息的方式。
- 在一个 LoWPAN 网络里发现资源的方式。

7.5.1 消息格式

在任何端口号下通过 UDP 转发 CoAP 信息，但优化 6LoWPAN UDP 压缩，使用 61616 和 61613 之间的端口号。图 7-12 给出了基本消息格式。通过 TCP 使用 TLS（传输层安全性）可保障 CoAP 的安全，但为了更好地加密信息优先使用 DTLS（数据报传输层安全性）[rfc4347]。

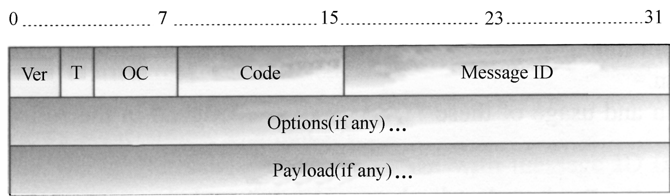


图 7-12 CoAP 头格式

消息包含以下字段：

● 两位的版本号，当前值是 1。

● 一个 T 字段（两位）给出消息的性质：

-0：表示一个确认消息（CON）；接收者必须确认。

-1：表示一个未确认消息（NON）；接收者需要确认。

-2：是确认消息（ACK）。

-3：是重置消息（RST）。

● OC（选择计数）是一个四位的字段，包含报头中的选项号，如图 7-12 所示，命令字段被限制，扩展报头需要选择字段，额外字段作为 TLV（类型/长度/数值）存储。采用这种方法，CoAP 报头转发仅适合特定行为的信息。

● 代码表示了消息的性质，在一个字节上进行编码，这可以看作是两个四位半的字节。在 HTTP[16] 中，状态代码是三位数的数字编码。1xx 是信息化的，除非考虑请求，不通知错误，并继续进行处理。2xx 表示成功，3xx 包括重定向，4xx 是由客户端发送的，通知错误，5xx 是由服务器发送的。因为在任何情况下，xx 比 15 要小，在一个字节里可以压缩编码，显示为 S. XX（这里 S 是 1 ~ 5 之间的值）：

-状态代码不等于 0，31 以下的值用于请求（O 表示无，1 表示 GET，2 表示 POST，3 表示 PUT，4 表示 DELETE），GET 允许客户端获取位于服务器的资源目录，POST 使用特定目录在服务器创建资源，PUT 在显存的资源中存储目录，DELETE 移动资源。

-32 以上的值用于应答。表 7-3 给出了错误代码，注意 HTTP 状态 200（OK）没有转化为 CoAP 代码，但 2. 05 可以用来代替。

● 消息的 ID 用于确认处理，CONfirmable 消息含有由发送者选择的唯一值，

ACKnowledgment 消息或 ReSeT 消息必须复制该值。

CoAP 使用一个简单的二进制头格式的异步传输的基础部分，其次是 TLV 格式的选项，数据报长度与消息有效载荷的长度相同。

表 7-3　应答值

成功通知代码			客户端错误通知代码			服务器错误通知代码		
65	2.01	Created	128	4.00	Bad request	160	5.00	Internal Server error
66	2.02	Deleted	129	4.01	Unauthorized	161	5.01	Not implemented
67	2.03	Valid	130	4.02	Bad option	162	5.02	Bad gateway
68	2.04	Changed	131	4.03	Forbidden	163	5.03	Service unavailable
69	2.05	Content	132	4.04	Not found	164	5.04	Gateway timeout
			133	4.05	Method not allowed	165	5.05	Proxing not supported
			141	4.13	Request entity too large			
			143	4.15	Unsupported media type			

为了简化解析，在基于类型的基础上，选项总是以相同的数值顺序发送。强制执行并在许多情况下减少类型字段的大小，只发送两个连续类型之间的增量。例如，如果一个消息包含选项类型 1、5、6、7 和 11，增量类型为 1、4、1、1、3。目前，定义的类型如下：

- 1（Content-Type）是参照一个 mime 值描述有效负载语法的值，例如，0：text/plain，44：application/soap + xml。
- 2（Max-Age）以秒为单位给出了最大持续时间，应答可以缓存。
- 3（Proxy-Uri）包含由代理服务处理的 URI。
- 4（ETag）用于检查在缓存和在服务器中的文件版本是否相同。
- 5（Uri-Host）、6（Location-Path）、7（Uri-Port）、8（Location-Query）、9（Uri-Path）和 15（Uri-Query）包含不同 URI 元素，由服务器简化解析。
- 10（Observe）用于从服务器接收定期更新值。
- 11（Token）用于与查询响应相匹配。

奇数表示一个重要的选项，这说明接收者知道如何对其进行处理，如果不是这种情况，会产生一个错误的代码。偶数表示被选中的选项，这说明如果不知道如何处理，接收者将忽略它。

在报头中，某些选项可能会多次出现，例如，在 URL 中路径由“/”隔开并分裂成片段，每段将被存储在不同的 URI 路径选项中。

在下面的章节中将介绍 TLV 的定义和使用。

7.5.2 传输协议

“传统”互联网中，TCP用于检测并纠正数据包丢失，吞吐量与网络和目的地能力相适宜。但是，TCP是一个非常复杂的协议，会产生大量的覆盖区，某些操作系统，如Contiki[㊀]，已经实现受限版本的TCP，其性能是有限的，因为传输窗口是设置为一个段。因此，为了避免这种额外的复杂性，CoAP依赖于UDP，但其执行自己的“传输”协议来纠正错误或重复。

基本协议使用消息ID字段跟踪消息，当发送CONfirmable消息时源地址选择唯一值，例如，无论何时发送新消息都使计数器递增，其中第一个值应该是一个随机数。如果接收者可以处理该消息，则发送一个ACK消息，或在其他情况下，接收者会发送含有相同消息ID的RST消息。

发送者跟踪已发送的消息并触发定时器，当发送者收到ACK或RST消息时，可以使计时器停止运行，并从存储器中移除与消息ID相关的消息，ACK消息也包含信息，在其他情况下，当定时器超时时，发送方将重新发送相同消息ID的消息。

图7-13显示了一些简单的例子。

在第一种情况下，发送者使用消息ID 0X1234发送CON消息，并且接收器立即确认该消息。在第二种情况下，该ACK消息丢失，然后发送者重新发送该信息，接收器应该注意到信息是重复的，因为消息ID是一样的，并不处理这个消息，但确认它停止发送方的定时器。

定时器值的设置是一个棘手的问题，因为节点中继的消息可以睡眠，传播延迟可能会很高并有一些大的变化，为所有类型的网络定义一个标准值，这是很困难的。默认值是2s，无论何时重新发送消息时，该值是翻倍的。经过多次尝试后（默认为4），发送方丢弃该消息。

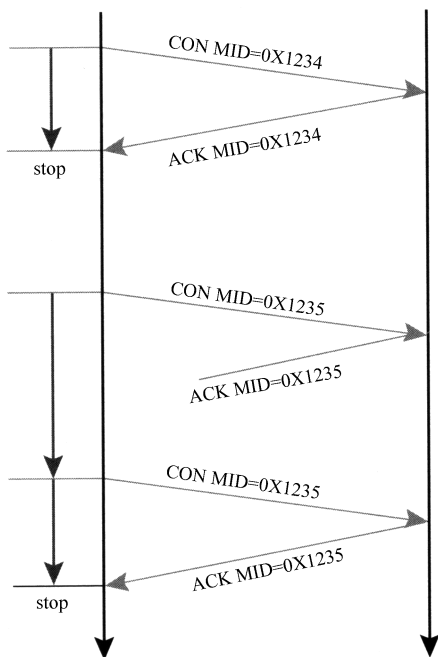


图7-13 CoAP传输流的简化例子

7.5.2.1 异步交换

图7-13描述的情况显示接收一个CON消息后立即发送ACK，很难延迟应答，因为

㊀ 见http：//www.sics.ce/contiki/。

它可以在发送方引发重传定时器的触发，但 CON 消息可能向接收者请求一个无法立即使用的值，一个标记选项（关键的值 11）可以用来映射应答查询。图 7-14 显示了标记选项使用的一个例子。

发送者发送一个请求的标记选项设置，接收者立即确认该请求，当接收器无法回复该查询时，发送一个含有应答的 CON 并等待对方的确认。

7.5.2.2　周期性的消息

有时，有必要定期探测传感器节点，以获得最新状态的信息，这可能是通过不断重复一个查询并等待回答而做到的。CoAP 定义选定的选项周期性的观测发送到一个单一查询的响应，选项观测与使用的标记有关，在查询与应答之间建立了连接。观测选项含有一个增加值，如果必要的话，允许发送者对消息进行重新排序。图 7-15 给出了一个例子。

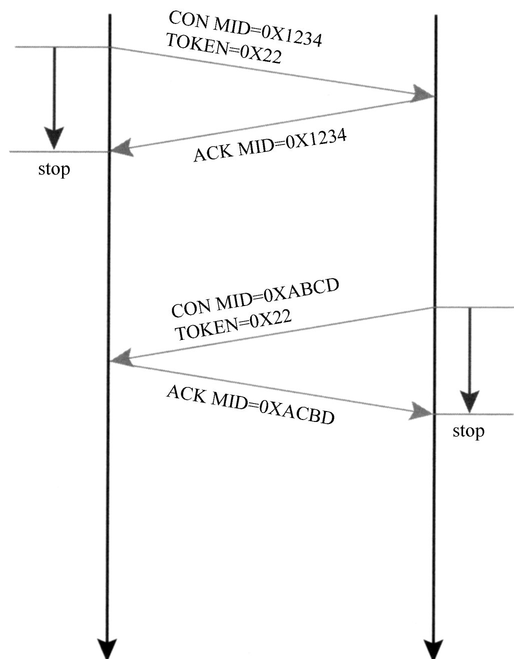


图 7-14　标记选项例子

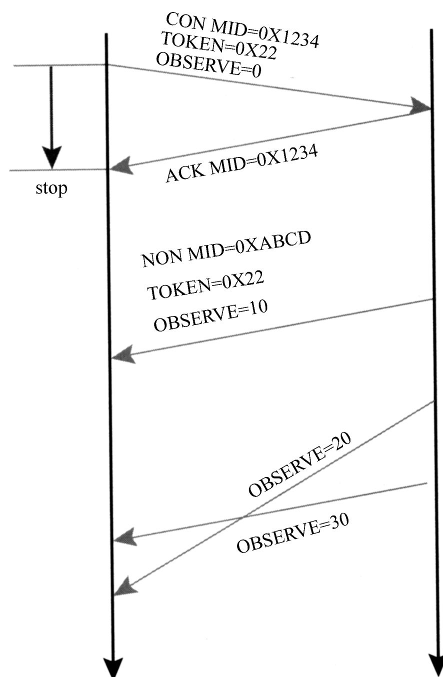


图 7-15　观测选项例子

发送器在请求中含有一个观测选项，如果接收器识别该选项，将返回周期通告。在这个例子中，它们将被送至 NON，因为周期性发送的损耗不是太重要。但也可以使用 CON，在此种情况下，必须发送一个新值，与前面的例子不同，这时必须停止重传尝试。

这个示例说明，通告的接收者可以用一个等于 20 的观测值选择忽略该通告，

因为在观测值设为 30 之前才接收到该通告。

要完成一个观测序列，启动该观测的设备要么在以 CON 发送观测的情况下可以发送一个 RST 消息，要么执行另外一个查询，而不使用观测选项。设备发送通告以错误消息而终止，或如果不能确认 CON 时则停止。

7.5.2.3　大数据块传输

在单一的消息中有时可以不发送请求或结果，多数文件的发送者可以使用块选项（关键的值 13）把它分解成更小的部分，该选项可以是一、二或三字节长，并且由 NUM 字段（4、12 和 20 位）组成，在文件中表明块号。当 M 位等于 1 时，表示必须发送更多的块，当等于 0 时，表示是最后一个块。最后三位包含块的大小（SZX），可以在两个实体之间进行协商，块的大小始终表示两个功率并由下式表示 block_size = 2^（SZX + 4），因此，该块的长可以是在 16 ~ 2048 字节之间。

块编号总是从 0 开始，且块总是以相同的方式进行确认作为消息。

在 GET 方法中，客户端不知道对应资源的大小，所以请求不包含块选项。服务器使用块选项应答，且服务器将使用该选项请求随后的块。

在 PUT 或 POST 方法中，客户端将直接使用块选项。

图 7-16 给出了块传输的一个例子。主机 A（REST 客户端的术语）给主机 B（服务器）发送 GET 请求获取资源/状态，忽略应答的大小，请求中不包含块选项。B 以请求文件的第一个块应答，B 发送第一个块（0）且 M 位被设置为 1，因为其他块将紧随其后。B 还选择一个大小为 128 字节（SZX = 3）的块，注意，数据被包括在该 ACK 消息里，也可以使用如前图所示的标记选项进行交换。

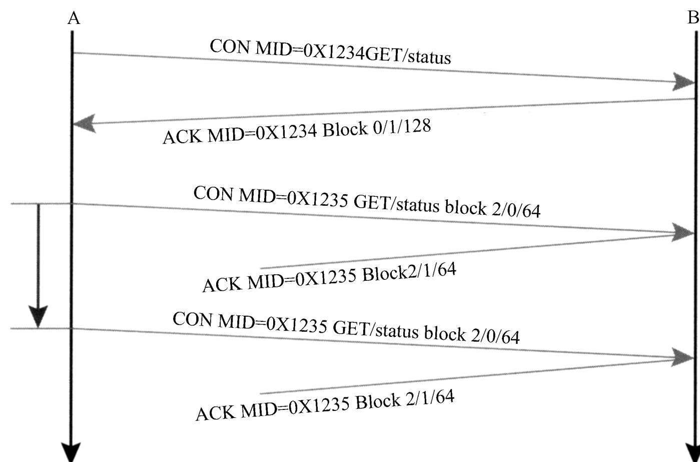


图 7-16　块传输例子

服务器 A 接收信息并请求下一个块，但由于其存储器限制 B 选择的尺寸太大，

所以 A 请求一个 64 字节的更小的块，改变块号以适应新块的尺寸，并设置 M 位为 0，因为没有任何更多的信息要发送。

在这个例子中，消息被丢弃，A 为其每个请求触发定时器，这种情况下，定时器超时，A 重发其请求。

7.5.2.4　多播

多播是一个非常有用的功能，例如，建筑物内同时切换几个灯。RLP 可以用于在 LoWPAN 中实现多播，但组管理可能需要大量有效的能量支撑整个网络。CoRE 工作组目前正定义在代理网关中基于应用水平实现多播的方法，属于多播组的任何节点都期望发送 CoAP 消息在网关中记录其地址，当网关发送消息至该组时，它将以单播的形式发送给所有成员。

7.5.3　REST 架构

通过 HTTP，REST 被广泛认为是网络体系结构模型，关于网络，RESTful 架构是非常适合于大多数类型的 M2M 应用，这是基于客户端 – 服务器模式的，该服务器包含的信息被保存或由客户端检索，在此实例中，传感器或驱动器可以被视为服务器和作为客户端的应用或网关处理。

请求是无状态的，这意味着一个请求始终与其他事项相独立。然而，服务器是有状态的，并可以通过请求更新，在客户端和服务器之间，允许请求被某些网关缓存或代理。

REST 在客户端和服务器之间定义了四个交互：

- GET（代码 1 在 CoAP 报头）：位于服务器上的客户端请求信息。
- POST（代码 2）：在位于服务器的一个源上，客户端创建和存储信息。
- PUT（代码 3）：在基于服务器的一个源上客户端存储信息。
- DELETE（代码 4）：客户端从服务器中删除源。

服务器上的源可以使用 URI 表示，其中包含用于接入该源的协议，服务器地址或名称随其后，并最终在该路径上服务器接入该源。

CoAP URI 可与 HTTP URI 相媲美，“coap” URI 用于在主机和端口内识别和定位 CoAP 资源，该资源以分层的方式组织并由 CoAP 服务器支配，这是通过普通的语法成分权限标识主机标识符和可选的 UDP 端口号，剩余的 URI 标识一个资源。路径由路径段序列组成，由斜线分隔字符“/”隔开。

CoAP URI 的语法是：

coap-URI = “coap:”“//” host [“:” port] path-abempty [“?” query]

应用设计人员需要在简略和叙述之间考虑 CoAP 环境受制于带宽和能量作一个权衡，例如，如果一个客户端使用这个 URI 查询服务器：

coap://sensor1.example.com:61620/external/temperature?max_value

它会产生一个消息发送到 61620 端口上的 IP 地址 sensor1. example. com。该 CoAP 消息包含：

- URI 主机 sensor1. example. com 选项。
- 两个 URI 路径选项，外部的在第一个，温度在第二个。
- max_ value 的 URI 查询选项。

7.5.3.1 HTTP 映射

在当前的版本中，代理可用于 HTTP 到 CoAP 的相互连接，或反之亦然。映射函数把 HTTP 字段转变成 CoAP 选项，由于这种转换是在应用级进行的，设备可以通过 DNS 名称指定，在 IPv4 和 IPv6 中的 CoAP 可能有 HTTP 请求。

该处理开始于使用 CoAP 中的"http" URI 代理 URI 选项请求 CoAP- HTTP 代理，或给 HTTP 发送 CoAP 请求反向代理映射 CoAP，该 CoAP 方法或响应代码，目录类型和选项被转化为响应的 HTTP 功能。有效负载并不需要任何转化，因为它可由两个协议以类似的方式实现。

图 7-17 给出了一个 CoAP 到 HTTP 的代理。

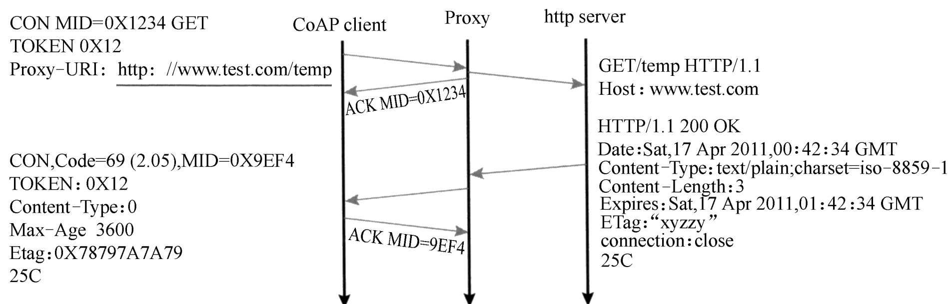


图 7-17 CoAP 到 HTTP 的代理

客户端向 CoAP/HTTP 代理发送 CoAP 消息，代理 URI 选项包含目标 URL http：//www. test. com/temp，此消息还包含一个与应答匹配的标记。

代理解析该代理 URI 选项中包含的服务器名称以获得服务器的 IP 地址，并开创了 TCP 连接，然后代理发送一个 GET 消息，其中包含绝对路径（/temp）和指定的 HTTP 版本。主机：在服务器端报头字段允许虚拟化。

服务器以一个包含报头和目录由空标题分离的 HTTP 消息应答，报头含有一个目录类型宣布目录以 Latin 字母表（ISO_8859_1）编码，代理把应答转换为 UTF-8，这将会更通用，因为它包含 ASCII 和 Unicode 编码。在一个 CoAP 消息中，值为 0 的目录类型与默认编码相对应，因此可以省略。到期 HTTP 报头字段转变成一个 max- age 选项，表示在缓存该目录和缓存一个含有信息标签的 ETag 需要多长时间（以 s 为单位）。

从另一种可选择的方案看到，为了在 CoAP 服务器中接入该资源，在互联网上的节点直接联系代理。图 7-18 给出了这种转换的一个例子。

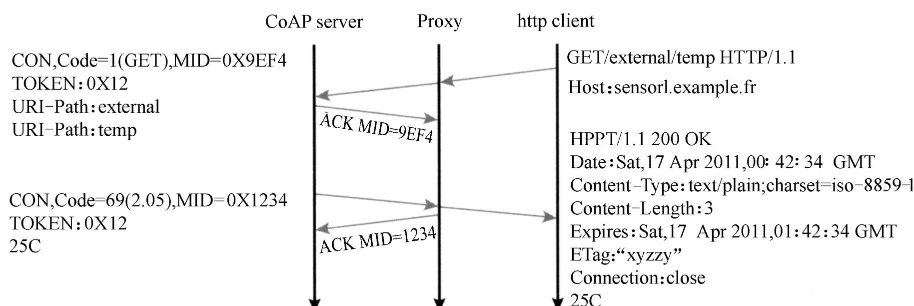


图 7-18　HTTP 到 CoAP 的代理

HTTP 客户端开启 TCP 与代理的连接并发送一个 GET 请求，其中包含想要探测的 CoAP 设备的主机名，代理解析该名称并发送一个 CoAP 消息，该路径分割成两条 URI 路径选项。CoAP 服务器应答值且代理把该应答转换为 HTTP 目录。

7.5.3.2　缓存

节点可以保持一个缓存响应，以减少延迟、网络带宽的使用和响应时间，但同时也需要一个新鲜度机制，可缓存的 CoAP 不依赖于请求的方法，但依赖于响应代码，除了以下几种情况，不使用存储响应：

- 用于实际请求的方法和用于获取一个存储的方法是相同的。
- 除了标记、max-age 或 ETag 请求选项，双方请求中的选项相同。
- 存储响应是新的或经过成功的验证。

新鲜度机制使用 max-age 选项，以确定请求是否可用于随后的请求而不与服务器联系，max-age 选项指定在几秒钟时间内，可以使用一个请求，其默认值是 60s。如果服务器不想使用缓存，则必须包含一个值为零的 max-age 选项。

当在缓存中有一个以上的 GET 请求响应时，结束点可以使用 ETag 选项选择一个存储响应并验证新鲜度。代码 2.03（有效的），在响应中确定，可以使用存储响应，并刷新 max-age 选项，任何其他代码将以一个发送取代存储响应。

7.5.3.3　资源发现

资源发现对于 M2M 的相互交流非常重要，这种交流循环中没有人的参与。已定义了一个著名的 URI，客户端可以使用它来决定服务器的功能，当客户端使用一条/.well-know/core 路径发送一个 GET 消息，响应负载基于 RFC5988 描述资源之间的链路消息格式，CoAP 响应包含以下属性：

- 字符 < >包围的路径显示在服务器获得资源的方式。

- rt（资源类型）描述资源的类型。
- 是否分配资源名称。
- ct 表示资源的目录类型，这是在 CoAP 选项中发现的相同代码。
- sz 返回资源的最大估计值。

要确定网络内部的资源，可以在多播进行查询。要限制应答的数量，可以在路径之后增加一个查询字符串，允许服务器执行这一功能来限制应答。

参 考 文 献

1. Briscoe, B., Odlyzko, A., and Tilly, B. (2006) *IEEE Spectrum*, IEEE, pp. 34–39, July 2006.
2. Postel, J. (1981) Internet Protocol. RFC 791 (Standard). Updated by RFC 1349, September 1981.
3. Postel, J. (1981) Transmission Control Protocol. RFC 793 (Standard). Updated by RFCs 1122,3168, September 1981.
4. Postel, J. (1980) User Datagram Protocol. RFC 768 (Standard), August 1980.
5. Tuexen, M. and Stewart, R. (2011) Stream Control Transmission Protocol (SCTP) Chunk Flags Registration. RFC 6096 (Proposed Standard), January 2011.
6. Kohler, E., Handley, M., and Floyd, S. (2006) Datagram Congestion Control Protocol (DCCP). RFC 4340 (Proposed Standard). Updated by RFCs 5595, 5596, March 2006.
7. Mockapetris, P.V. (1987) Domain Names – Implementation and Specification. RFC 1035 (Standard). Updated by RFCs 1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, November 1987.
8. Deering, S. and Hinden, R. (1998) Internet Protocol, Version 6 (IPv6) Specification. RFC 2460 (Draft Standard). Updated by RFCs 5095, 5722, 5871, December 1998.
9. Montenegro, G., Kushalnagar, N., Hui, J., and Culler, D. (2007) Transmission of IPv6 Packets Over IEEE 802.15.4 Networks. RFC 4944 (Proposed Standard), September 2007.
10. Narten, T., Nordmark, E., and Simpson, W. (1998) Neighbor Discovery for IP Version 6 (IPv6). RFC 2461 (Draft Standard). Obsoleted by RFC 4861, updated by RFC 4311, December 1998.
11. Savola, P. and Haberman, B. (2004) Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address. RFC 3956 (Proposed Standard), November 2004.
12. Dohler, M., Watteyne, T., Winter, T., and Barthel, D. (2009) Routing Requirements for Urban Low-Power and Lossy Networks. RFC 5548 (Informational), May 2009.
13. Pister, K., Thubert, P., Dwars, S., and Phinney, T. (2009) Industrial Routing Requirements in Low-Power and Lossy Networks. RFC 5673 (Informational), October 2009.
14. Brandt, A., Buron, J., and Porcu, G. (2010) Home Automation Routing Requirements in Low-Power and Lossy Networks. RFC 5826 (Informational), April 2010.
15. Martocci, J., De Mil, P., Riou, N., and Ver-meylen, W. (2010) Building Automation Routing Requirements in Low-Power and Lossy Networks. RFC 5867 (Informational), June 2010.
16. Fielding, R., Irvine, U.C., Gettys, J. *et al*. (1999) Hypertext Transfer Protocol – HTTP/1.1. RFC 2616, June 1999.

第 8 章　M2M 的安全性

Ioannis Broustis，Ganesh Sundaram，Simon Mizikovsky，Harish Viswanathan
阿尔卡特朗讯公司，新泽西州，美国

在任何数字通信环境中，安全性都具有举足轻重的作用，尤其在机器对机器（M2M）无线通信领域，安全的作用尤为重要。一些现有的服务基础设施，例如蜂窝系统中，典型的服务、网络和设备分布紧密结合，并且由网络运营商，这一单一实体进行管理。另一方面，M2M 解决方案通常涉及多个实体，如应用提供商、网络运营商和众多的设备制造商。所有这些实体之间可能会以多样化的方式进行关联，其中某些实体将无法再被关联。换句话说，在 M2M 环境中，由于各方可能并不直接交互而建立正式的业务关系（包括信赖关系），因而存在着复杂的信任关系，这一根本问题，需要提供一些新颖的、具有可扩展性和自动化的方法来设立安全协会。这样的方法应该是能够利用多种接入网络技术处理一些 M2M 设备和由一些 M2M 运营商提供的数百个应用中存在的潜在的爆炸性危险的手段。

在本章中，详细地阐述了各种 M2M 实体之间复杂的信任关系。这种复杂的信任关系也为设计 M2M 安全策略和解决方案以及避免出现设计缺陷提供了指导性的思路，此外，本章还讨论了各种安全策略如何纳入 M2M 系统以防范系统潜在威胁的问题，另外，本章还对正在进行的标准化工作情况进行了简要介绍。

8.1　引言

M2M 市场高度分散，许多参与者横跨众多垂直领域，另一方面，该行业利用 M2M 服务价值提高企业生产力，以及广泛考虑消费者的便利和舒适。考虑到大型网络运营商集中于 M2M 的应用增加其现有资产，再加上开放它们的网络和设备，M2M 通信以前所未有的方式蓄势待发。通信安全是 M2M 的大规模市场应用的关键推动者，终端用户需要 M2M 通信至少达到如传统人类通信相同的安全级别。在数字化背景下，保密性、完整性保护、隐私、身份验证和授权是安全的一些关键要素，需要以端对端的方式进行处理。

现已在多种不同环境中部署了一些 M2M 服务系统，特别是，目前的蜂窝网络用于许多 M2M 解决方案。在本章中，我们将重点放在蜂窝 M2M 通信情况下的潜在安全解决方案的适用性评估。下面一节讨论蜂窝 M2M 系统的固有特性，该系统

具有某些不适用的安全策略。

8.1.1 蜂窝 M2M 的安全特性

蜂窝 M2M 在三个重要的方面不同于当前的蜂窝网络，这表明这种网络中适用于当前移动设备的现有安全机制不适合于 M2M。

首先，今天的蜂窝网络服务通常由单一服务提供者提供，服务提供者通常拥有连同 SIM 卡分布、设备供应、网络基础设施、语音和数据服务的服务配送的设备分布。在某些情况下，设备分布、设备供应和设备配送由一个移动虚拟网络运营商（MVNO）所拥有，而底层的网络基础设施由不同的网络供应商所拥有。另一方面，蜂窝 M2M 的多个参与者与他们之间限制性的商业关系共存。

8.1.1.1 使用实例

我们考虑这样一种场景作为例子，一个公用事业公司计划采用蜂窝无线调制解调的连接部署智能电表。实施这一方案的方法之一是典型的 M2M 服务，公用事业公司从电表制造商订购电表，并订购 M2M MVNO 的 M2M 服务，该服务已与多个蜂窝运营商协商了网络接入和相关的服务。公用事业公司获取和部署电表，同时在他们的数据库中配置，并在 MVNO 数据库中提供连接服务。涉及提供解决方案的实体是这样的：公用事业公司，这是这个实例的应用提供商，为此目的征募 M2M 运营商、蜂窝接入网络提供商、电表制造商和终端用户。注意，部署设备的公用事业公司和蜂窝接入网络提供商之间并没有任何关系，换句话说，这两个实体并不需要相互信任。因此，在这样一个开放的和断连的商业环境下，采用的安全解决方案应该是可行的。

第二个重要的区别是由于这样的事实：在许多 M2M 应用中，存在大量的设备，每个仅贡献少量的数据，并由此从每个设备到涉及的各类参与者都产生相对较低的收入流。M2M 的经济性不允许采用与蜂窝手机类似的安全配置过程，一个简单的自动化过程有效地处理大量设备制造商的能力是理想的。在上述的使用情况下，一个期望的部署过程将是简单地直接从制造商到终端用户运送仪表，在一般情况下，传送到站点之前，通常不能定制 M2M 设备，它们是收缩包装的翻版，潜在的差异仅在于其独特的媒体接入控制（MAC）和电子序列号，该设备通常安装于多重时间框架之上，并应无缝集成于网络之中。此外，该安装通常是由终端用户或拥有少量通信工程经验的承包商去做。

最后，与移动电话、智能手机或带无线支持的笔记本电脑不同，M2M 设备往往无人值守并受到破坏和滥用的风险较高。特别是，使用 M2M 设备对其他应用的威胁，如网页浏览是一个真正的风险，这样的篡改可能涉及没有授权接入设备的用户。可适用的安全解决方案的设计应防止这种对设备的不恰当使用，随后保护网络运营商和 M2M 应用提供商。

此外，在蜂窝 M2M 背景下，我们正在处理由设备数目（可能运行到数十亿美元）和一些虚拟运营商使用混合接入网技术提供的数百个应用。因此，我们期望众多设备供应商参与相对开放的系统直接向消费者或通过应用提供商销售低成本设备。例如，用户在开放市场购买设备，设备制造商和 M2M 服务提供商可能没有业务关系（因此没有预定义的相互信任）。另外，在住宅应用领域，如计量，终端用户（家庭所有者）可能甚至没有意识到存在虚拟网络运营商，其提供服务代表该组织所有者拥有的应用。然而，确保应用是链条中所有参与者的关键所在。

8.1.1.2　样本攻击

在下面的例子中，我们将讨论两种可能的 M2M 设备的攻击，同时考虑到 M2M 系统部署的固有特性。我们特别考虑蜂窝网络的连接，其攻击也容易应用于其他网络技术。

例 1：可撤销证书的盗窃

在这个例子中，攻击者从一个 M2M 健康监测 M2M 设备中提取（可拆除）通用集成电路卡（UICC）模块，并将其安装到一个智能手机中。考虑到 UICC 是合法的，移动接入网络会成功注册，并授权智能手机接入网络服务。这是因为移动终端注册网络所有必要的信息位于 UICC 内。换句话说，该网络无法明确识别带有 UICC 的移动设备。这种攻击的结果就是攻击者可以使用智能手机来浏览网页，计费标准是按 M2M 设备订阅对应的计费率，所以这可能是相当便宜的（甚至免费，这取决于用户、M2M 运营商和网络运营商之间的关系）。更重要的是，接入网络运营商根据网络订阅的数量和类型的基础上，仔细规划他们的网络提供一定数额的流通。任何恶意使用 M2M 设备接入未经授权的服务完全歪曲了这样的网络规划，导致对合法的终端用户的劣质服务。在类似的情况下，在 M2M 设备不能进行物理接入时，攻击者不得不盗窃 M2M 设备的接入凭证，如 IP 地址和在注册过程中网络临时分配给该设备的标识符，例如在码分多址（CDMA）的 1xEV-DO 网络[1]的情况下单播接入终端标识符（UATI），在 UMTS/HSPA 网络也是一样的。在这种情况下，攻击者可能会试图给合法的数据对象注入数据包，这个数据对象是由网络在受害者的 M2M 设备中创立的。

对可移动凭证（如在可拆卸 UICC 的情况下）的物理消除和使用会有以下的影响：

- 交互网络身份验证过程中验证 UICC 中的凭证。因此，不考虑承载 UICC 的设备，注册过程中将会验证 UICC 的有效性并成功地授权设备使用网络服务。注意，这个问题存在于任何一个带有 UICC 的普通移动设备中，因此它不是 M2M 设备所特有的。

- 所有临时身份凭证和相关的网络配置参数将会为带有合法的 UICC 设备生成，也就是说，攻击者的智能手机设备也能生成。换句话说，目前授权网络还没有

办法去把智能手机从 M2M 设备中区分开来。只要该设备带有一个合法的 UICC，该设备就会被授权接入网络服务。

● 攻击者甚至可能拥有一个恶意的带有 UICC 的 M2M 设备。在这种情况下，攻击者不必试图物理接入属于别人的 M2M 设备。例如，攻击者可以将 UICC 从他/她的健康监测设备分离出来，并把它安装到一个智能手机上。导致这种行为的原因可能是对应的 M2M 业务的接入网络运营商的计费率远远低于普通的 3G 数据连接。此外，对于附属的 M2M 服务器很难发现它们被滥用，因为互联网的流量请求不会通过 M2M 服务器路由。

● 即使接入网络供应商已启动加密和完整性保护，一个外来合法的 M2M UICC 的使用能够完全不被发现。这是因为那些用于加密和完整性保护的密钥在每一次新注册时都会被更新。因此，对抗式的移动设备将能够产生这样的密钥，因为它会带来一个合法的 UICC。在使用这些密钥时，源于此设备的数据包将会被正常加密和潜在的完整性保护。

例 2：通过无源媒介偷听拦截攻击

即使在缺少 UICC 的情况下，通过简单的偷听 M2M 设备和接入网之间的控制和数据通信，攻击者可以劫持 M2M 蜂窝网络连接。攻击者的目的是使用合法的设备认证，才能自由地接入网络服务。作为一个例子，我们假设攻击者希望建立一个与远程主机的 UDP 连接，上行方向的数据流（例如，视频流量）作为基于 EDVO 接入网络的情况（攻击也同样适用于其他技术）。攻击者能够自由地使用如下所示的上行链路业务信道：

● 攻击者偷听 M2M 设备（M2ME）和无线网络控制器（RNC）在注册过程中的所有数据包之间的交流，所有这些信息是不加密的，因此，服务系统指定的用户设备的特殊无线信道识别对空中接口起作用，攻击者已知所谓的 UATI 和 IP 地址。

● 攻击客户端设备中的应用层上产生视频帧，例如，通过一个网络摄像头应用，每一个这样的帧被转发到 IP 层，在那里它被封装到 IP 层分组，IP 封装功能已被攻击者修改，包括：①偷听 IP 地址作为 IP 源，②攻击者所需的远程主机 IP 地址，作为 IP 目的地。

● 每一个片段被转发到 MAC 层，其中添加了 MAC 报头，这个报头包括偷听 UATI24（24 位的 UATI 编码）值，物理层（PHY）使用对应于所分配的 UATI 的长码传输每个 MAC 帧到基站，由于攻击者已知 UATI，后者能够重建该长码对应于偷听 UATI。对于每个片段传输，上行链路业务信道由 RNC 在使用建立连接期间被分配给 M2ME。

● 基站向 RNC 转发每个片段，融合片段，以便重建 IP 层分组。如普通的 RNC 实现，为了识别始发 M2ME，通过 UATI24 值，RNC 检查每个片段的 MAC 报头，然后使用 A10 接口，将该值用于查询本地维护（UATI24——通用路由封装（GRE）

键）组合，以打开 IP 数据包到分组数据服务节点（PDSN）的通道。GRE 键标识一个特定的与一个特定用户会话相关联的 A10 信道（或 GRE 通道）。注意，在这里，RNC 接收片段含有合法的 UATI 值，因此，RNC 被交给“信任”片段，该片段是由设备最初请求特定的 UATI 分配发送的。

● PDSN 从 GRE 通道收到 IP 数据包并咨询其本地维护查找表以验证源 IP 地址实际上对应于所使用的 GRE 键，只要条目被验证，该数据包被发送到攻击者预定的目的地。对于这一点，使用数据包的目的 IP 地址，显然，PDSN 没有进一步质疑数据包有效性的依据。源 IP 是一个合法的地址，在注册过程中被分配给 M2ME，并对应匹配的 GRE 键。

● 假设攻击者总是可以从无线接入网络（RAN）向受到侵害的 M2ME 偷听信令消息和命令，攻击者总是可以响应这样的命令，或者是使用其自己的信任证，或者是使用偷听的凭证，显然，攻击者不需要总是位于邻近 M2ME 的位置，但需要可选择地与基站相接近。

第二个例子说明，攻击者只需要偷听接入网络运营商分配给 M2ME 的 UATI 和 IP 地址，使用这些值，攻击者可以产生“误导”接入网络的数据报头信任从一个合法客户端始发的数据包，注意，攻击者需要同时使用特定的偷听 UATI 和 IP 地址（分配相同的合法 M2ME），只有这些值中的一个是不够的，因为：

● 如果使用一个不同的 UATI，它将对应于一个不同的长码和一个不同的 GRE 键。假设这个 UATI 确实存在，它会误使 RNC 使用不同的 GRE 通道，然后 PDSN 将拒绝该数据包，因为在使用的 IP 地址和 GRE 键之间存在不匹配。

● 如果使用不同的 IP 地址，因同样的原因 PDSN 将拒绝数据包：PDSN 在其本地存储查表中将不会识别任何有效的（GRE 键-IP 地址）元组。

因此，为了保证攻击的成功，UATI 和 IP 地址（分配给相同的 M2ME）都需要被偷听。

显而易见，目前的接入网络将携带合法 UICC 授权接入任何设备，换句话说，蜂窝接入网络没有办法检测这类劫持攻击。

在本章中，我们主要阐述蜂窝 M2M 系统，识别出所有不同的业务实体以及涉及其中的安全信任关系。此外，介绍 M2M 安全相关的标准化工作。另外，讨论 M2M 服务的安全性要求，并进一步评估现有安全方案是否适合于 M2M。

8.2　M2M 生态系统中的委托关系

传统的网络服务，如移动语音和数据服务，由运营商提供，部署和运营网络、市场服务、认证和开通设备与终端用户的信道，并管理终端用户的订阅和计费。从本质上讲，一个单一的实体涉及每种设备的各个方面。另一方面，M2M 服务通常涉

及每种服务交付的多个实体，最常涉及的实体是终端用户、网络提供商、M2M 服务提供商、应用软件提供商和设备制造商。M2M 运营商从多个网络提供商批量协商网络服务，并代表许多应用提供商管理网络接入订阅。应用提供商，顾名思义，是提供终端用户应用的实体，如收集和处理数据。一个终端用户可以从制造商（通过零售分销网络）或从应用提供商直接购买包含网络连接模块的设备。因此，生态系统比传统网络服务复杂得多，这使得高效的端到端安全解决方案的设计非常具有挑战性。

有多种原因使得 M2M 服务交付生态系统更复杂：

●鉴于 M2M 通信的范围，许多设备制造商正参与一个开放式的生态系统，这意味着应用提供商与制造商之间可能有关系，也可能没有关系。在这种情况下，它们之间没有预定义的信任关系，因此应用提供商不能纯粹依靠制造商提供的安全解决方案，特别是面向大众市场的应用，单独的机器保守通信，维护设备分销供应链会使应用提供商产生额外费用。相反，对于高端、小批量、高价值的应用，如急性健康状况监测，应用提供商有理由使终端用户拥有单个设备分布。

● 许多 M2M 服务的一个重要要求是需要保证网络在许多地区的连接性，因为对于一个给定的应用客户可以跨越大片区域，即使一个给定的网络提供商可能是区域性的。这需要使用多个属于独立的网络提供商的接入网络。此外，某些处理，如业务开通、计费和设备管理，是如此显著地不同于 M2M 服务，与人工服务相比，如手机，装备不良的传统网络提供商经济地执行这些过程。这导致了 M2M 服务提供商需要在应用提供商和网络运营商之间提供桥梁关系。显然，应用提供商始终维护客户和 M2M 服务提供商之间的业务关系，同样，M2M 服务提供商与一个或多个接入网络运营商之间存在关系，当接入网络运营商本身可能是 M2M 服务提供商时，我们重点集中在这样的情况，从客户的应用提供商的角度来看 M2M 服务提供商是一个独立的实体。

● 该设备可由终端用户客户使用，他可能不具有设备的所有权。此外，由于保持设备成本低的固有工作，对于客户交互设备，用户界面不会一直存在。

下面用例子说明在 M2M 服务交付中涉及的业务关系。第一个是智能电表，在这个例子中，一家电力公用事业公司将从电表制造公司购买智能电表，并把它们分发给预订该实用服务的终端用户，在终端消费者的前提下，该公用事业公司将拥有和部署该仪表。公用事业公司从 M2M 服务提供商订阅 M2M 服务用于电表数据采集和设备管理。M2M 服务提供商，于是与网络提供商具有使用带宽传输数据的业务关系。表 8-1 显示了不同的实体和它们之间的关系。

为了进行比较，表 8-2 显示了传统蜂窝语音服务情况下所涉及的关系。表的对比显示，表 8-2 中的许多实体是无效的，这表明一个更简单的生态系统。

第二个用例，车队管理，如表 8-3 所示。在这项服务中，应用提供商向小

表 8-1　智能电表服务中主体之间的业务关系

	角　　色	消　费　者	设　　备	网络服务提供商	M2M 运营商	应用提供商
消费者	订阅实用	—	—	—	—	—
设备	智能电表的无线模块	安装在用户的处所的装置	—	—	—	—
网络服务提供商	提供移动通信	没有	在设备中认证无线模块	—	—	—
M2M 运营商	为设备提供家庭网络，并为多个传输网络提供商提供连接的虚拟网络运营商	没有	没有	漫游关系	—	—
应用提供商	提供了智能电表应用和服务的实企	消费者订阅的跟踪服务	公用事业实体所拥有、所部署的设备	没有	应用程序订购的与 M2M 运营商的连接服务	—
设备制造商	制造设备并集成无线模块	没有	制造设备	没有	没有	制造商为公用事业部署提供设备

表 8-2 语音服务中主体之间的业务关系

	角　　色	消　费　者	设　　备	网络服务提供商	M2M 运营商	应用提供商
消费者	订阅语音服务	—	—	—	—	—
设备	手机	消费者拥有的设备	—	—	—	—
网络服务提供商	提供移动通信	提供设备	认证设备	—	—	—
M2M 运营商	不存在	没有	没有	没有	—	—
应用提供商	与网络服务提供商一样	没有	没有	没有	没有	—
设备制造商	制造设备	没有	制造设备	批发供应商	没有	没有

表 8-3　车队管理服务中主体之间的业务关系

	角　色	消　费　者	设　备	网络服务提供商	M2M 运营商	应用提供商
消费者	从应用程序处订阅跟踪服务	—	—	—	—	—
设备	跟踪服务	消费者从零售商处购买的现成设备	—	—	—	—
网络服务提供商	提供移动通信	没有	在设备中认证无线模块	—	—	—
M2M 运营商	为设备提供家庭网络，并为多个传输网络提供商提供连接的虚拟网络运营商	没有	没有	漫游关系	—	—
应用提供商	为中小型企业提供车队管理服务	消费者订阅的跟踪服务	没有	没有	应用程序认购的与 M2M 运营商的连接服务	—
设备制造商	制造设备	没有	制造设备并通过零售网点销售	没有	没有	没有

型和中型公司提供车队跟踪和调度服务，该服务不同于智能电表的例子，主要在于终端用户从零售点购买设备，并自己拥有和部署，而不是由应用提供商进行。

总之，M2M 生态系统涉及潜在的十亿客户（每个用户通常有一个以上的设备）的通信并由数以千计的应用提供商提供支持，它们之间通常保持信任关系。这些应用提供商与少量的 M2M 服务提供商一起工作，反过来可能维护多个网络运营商的业务关系。该设备生态系统包括许多制造商通过零售网点到达客户，或利用应用提供商拥有的分销渠道。

鉴于上述情况，我们注意到，M2M 生态系统的复杂性的突出特点是多样化的业务（或信任）关系，在安全解决方案的设计过程中，不能准确地预测。因此，M2M 系统的安全协议设计内在的假设 M2M 服务提供商可能与生态系统中的其他利益相关者之间没有信任关系。在以下几节中，我们将评估 M2M 案例的各种安全策略的适宜性，并提供适用的安全解决方案的设计建议。

8.3　安全要求

从需要防止端到端的各种实体感知到威胁，制定 M2M 安全要求，我们将提供由前面章节中被识别的每个参与者所经历的威胁的例子，然后总结安全要求。

8.3.1　客户/M2M 设备用户

攻击者假装是后端应用服务器，可以劫持设备为他们提供数据，或成为他们的驱动能力。该攻击可能是这样一种情况：对于攻击者，一些具有经济价值的攻击是家庭自动化设备的远程控制，如报警和车库开门器。通过假装是基于网络的家庭自动化服务器，攻击者可以禁用警报，并打开大门进入屋内。硬件设备必须防止未经授权实体试图建立与该设备的通信。

许多 M2M 应用的 M2M 设备收集到的数据实质上是敏感的，例如，在一个儿童跟踪应用中，一个未经授权的人获取孩子的位置信息应该是不可能的。因此，M2M 安全解决方案必须是这样的，在网络中的任何地方，通过窃听都没有可能获取所存储的数据的有关信息。

身份是一个有价值的信息，因为它与其他数据有关，如检索该身份信息识别某些模式的网络元素的位置，在某些应用中，重要的是，终端用户的身份是不可用的。因此，未加密的传输设备的实际身份是不可接受的，因为在网络中，设备或其用法可以被攻击者窃听跟踪。

8.3.2　接入网络提供商

与消费类电子设备的情况不同，M2M 设备在许多情况下由应用提供商所拥有并部署在不经常使用物理监视或保护的场所。例如，在智能电表的例子中，电表通常由公用事业公司拥有并部署在家庭和小型企业场所。因此，这些器件更容易被盗，为了规范互联网通信（如网页浏览）的目的，滥用偷窃的这些设备中的通信模块是不应被允许的。

M2M 劫持的背后，攻击者使用合法设备证书自由接入网络服务，也威胁着接入网络运营商。甚至可以在非 M2M 设备（如常规智能手机、PDA 等）使用智能化的恶意软件启动该类攻击，在 M2M 布局中，这种情况更为突出，这是因为两个固有特性使 M2M 设备易于发生以下的攻击：

● 低廉设备：一个低成本的心脏检测设备只是测量每分钟的脉冲数，并通过蜂窝网络连接把这些信息发送给远程服务器。这类设备通常没有更多的功能和任务。同样，家庭智能仪表在一个测量周期内测量所消耗的水量，并把此信息报告给自来水公司。在这两个例子中，M2M 设备和预定义的服务器之间建立了一个数据对话；设备不需要连接其他任何实体。因此，这类设备自然便宜，这将使聪明的攻击者很容易侵入此类设备并破解。

● 存取的便利性：可能的 M2M 部署主要由静态（或可能是移动性非常低）的设备组成，放置在可视的且物理接入的位置。从安全性的角度来看，期望有两个使情况复杂化的因素。首先，若其存储在一个可移动的卡（例如 UICC）中，并安装嗅探器，以及执行其他可采取的行动，攻击者能够物理接入该设备、删除/更换凭据。其次，在一个静态设备安装中，不同基站或 RAN 没有越区切换，攻击者可以很容易地确定附属接入网络的身份以及所分配的临时 M2M 设备的身份。

8.3.3　M2M 服务提供商

M2M 服务提供商的威胁包括适用于网络运营商的所有情况，此外，M2M 运营商的责任是确保应用提供商的服务的可用性，并保证发送到应用提供商数据中心的数据不被篡改。

8.3.4　M2M 应用提供商

通过中间人攻击，对由设备传向后端应用服务器的数据进行篡改，攻击者可能因此而获益，反之亦然。这样，验证实体之间传输的数据的完整性应该是可能的。

某些设备可能会伪装成其他设备，即模拟网络中的其他设备并向后端服务器上

传数据。例如，在智能计量服务中，它的仪表数据是从各种仪表收集来的，不诚实的房主可能改变仪表识别，使应用服务器看来是邻居的仪表，从而逃避使用电力的支付。另一种可能的威胁是攻击者伪装成合法的设备给服务器发送虚假信息，例如，在一个囚犯跟踪服务中，另一台设备可以充当像囚犯的设备，谎报位置，而合法设备却被破解，甚至被破坏。

基于上述威胁，对于任何安全解决方案，我们可以得出以下的共同需求。

● 双向认证：只有经过身份验证的 M2M 设备可以接入网络和 M2M 系统，反之，任何 M2M 设备在接收任何数据之前都需验证服务器，如指令或相关的管理更新。这将确保后端服务器所收集的数据是来自于合法的设备，且确保该设备与合法服务器的通信。在开始传输数据之前，双向认证程序必须在 M2M 设备和 M2M 运营商网络之间完成。

● 保密性：M2M 设备和应用服务器之间的数据传输应受到保护，避免来自未经授权的窃听。

● 完整性：应用服务器应该能够验证来自于相关设备的数据的完整性。同样，设备应该可以验证附属服务器发送的数据的完整性。这可以保护数据以免未经授权的修改或操作。

● 独特性：机器模块的通信设备不应用于其他应用，当网络提供商实体和应用提供商实体分开时，这一要求意味着，网络提供商必须拒绝服务篡改的设备。

● 匿名：在网络中，设备的身份不应该透露给窃听者。

此外，在引导安全解决方案中存在下列需求，这些需求是专门针对于 M2M 通信的。

8.3.5 需求引导

在 M2M 生态系统中，我们正在着手解决激增的设备数量（如果普遍采用，也许会飙升到数十亿台）和一些虚拟运营商使用不同的接入网技术提供的数以百计的应用，因而，一些制约因素被强加在安全密钥的引导指令中：

● 复杂的生态系统：我们期待众多的设备提供商参与相对开放的生态系统，直接向消费者出售低成本设备。

－如前所述，复杂的生态系统可能需要设备制造商在一个开放的市场销售，而服务提供商可能与设备提供商或经销商没有商业关系。

－另外，在住宅应用领域，如计量，终端用户（房主）可能甚至不知道提供服务的虚拟网络运营商代表拥有应用的机构所有者，但还确保应用对链接中所有参与者是关键的。

● 扩展性：M2M 服务通常涉及大量的设备，每台设备发送少量的数据，在价值链中对于任何参与者，每台设备的收益都比较小。因此，重要的是尽量减少部署

和维护这些设备所带来的费用。设备部署的关键步骤之一是在网络和应用提供商的相应数据库的设备供应。特别是，配置的密钥或其他信息的安全解决方案应该是简单和可扩展的，该配置过程假设在一个已知的、预先安排的具体时间里，不能将该设备激活，在制造现场设备可被暂时接通用于测试，但随后部署时关闭，可以在同一个时间进行安装，但只能稍后接通通信。因而不能预测供应过程执行的特定时间。考虑到生态系统中设备的体积，引导应用应尽可能自动化，事实上，在许多情况下，任何人工干预（离线或其他方式）应仅限于消费者或安装者用键盘输入数据到一个在线数据库（如果需要的话），或在设备中使用命令线型接口。

- 引导需要网络身份验证：更重要的是，当设备正在执行引导应用时，网络运营商（给 M2M 运营商提供带宽）极有可能无法显示。例如，该约束条件要求设备使用网络接入身份验证自身与移动数据网络，这允许网络运营商识别该设备并授权该数据交易，尽管移动设备还没有拥有安全密钥或其他接入凭证。换句话说，M2M 设备的引导协议应假设 M2M 系统是覆盖现有（和部署）网络系统，因而需要设备在调用引导应用之前就以接入网络成功注册，且这样的注册程序应明确符合现有的网络标准。
- 运营商选择的灵活性：除了本节之前所述的要求之外，还存在另一种情况：在某个时间点（由于各种业务缘故），应用提供商可以选择切换 M2M 运营商。反过来，要求任何引导程序必须提供完善的前向和后向保密性，不泄露运营商的关键资料。另外，须尽量保证该要求没有人为干预。

由于这些限制，才得以确保整体引导问题符合安全要求，并在设备、链路、网络或应用层不存在破解。

8.4　哪些类型的解决方案是合适的

对于其他类型的部署已经提出了各种的攻击检测和预防计划，下面我们对其进一步地扩展。

8.4.1　阻止黑客行为的途径

8.4.1.1　加密和完整性保护

大量研究及相关标准都提出使用加密操作以检测和防止劫持攻击[2-15]。概括地来说，这些研究中提出的最重要的思想是保护控制和数据信息的完整性：①使用仅由会话参与者知道的密钥散列数据包内容及②在消息的末尾附加散列操作的结果。接收方可以使用相同的密钥来产生散列结果，并与在接收消息中附加的结果相比较。如果它们匹配，则接收方确信消息的真实性。借助该方法，当攻击者设法获得除设备身份之外的共同密钥时，劫持是唯一可能的途径。与提供完整性保护一样，

保证数据传输的加密确保设备身份以防欺骗。但在某些情况下，必须发送未受保护的设备身份。此外，在操作处理方面，许多这些加密操作开销是极其密集化的[16]，并且这样的处理对于低廉的 M2M 设备价格过高。有研究建议，用户数据流量包本身具有不完整性保护。在实践中，当广泛使用用户数据加密的同时，用户流量的完整性保护增加了 RAN 的巨大开销，从而不支持蜂窝网络标准[2]。在另一方面，控制信令是典型的完整性保护，由于有限数量的信令消息和分散性质，即使完整性保护强加大量开销也不会严重影响网络性能，因此控制信令得到广泛使用。

8.4.1.2 基于 IP 地址的滤波

该技术的主要思想是在中间的路由器上沿着路由路径检查数据包的源 IP 地址，以便检测冒名、反射和隐藏攻击。此技术包括使用路由表检查传入的数据包并查找源 IP 地址的返回路径，及把已分配的 IP 地址与特定 MAC 地址相比较，可能通过 IPCP 或 DHCP[17]来实现。但在我们的研究范围内，该技术还存在不足之处，因为：①攻击者的设备可能位于与受害者设备非常近的地方；②在设备登记程序中，源节点的身份（不管是临时的还是永久的）也能很容易地被偷听，我们在下面的章节将进行详细说明；③根据 RAN 实现，来自于客户端设备的数据包可能不包括任何设备身份。另一个工作机构使用 IP 地址信息来执行流量特征监听和分类，这种机制的主要目标是通过观察某些客户端设备是否已经被入侵，从而检测网络异常，即检测相关的流量特征是否已改变。例如，是否正在使用新目的主机，是否正在推出不同类型的流量，这种机制的提出都主要用于检测蠕虫攻击。但这种机制在检测 M2M 劫持中效率比较低，因为一个精明的攻击者可能使用一组非常大的数据偷听 IP 地址并以随机方式临时识别。由此，流量监听器/分类器不能有效地识别任何恶意流量，因为这被均匀分布在显见的众多合法源节点。

在满足上一节中所讨论的安全要求的基础上，我们在下面的章节中讲述现有的用于 M2M 安全引导和建立安全会话的可用解决方案，以评估其是否适于 M2M。

8.4.2 公钥解决方案

用于引导密钥的一个众所周知的方法包括配置一对私钥和公钥以及公钥证书[18]。这对密钥可以单独在制造过程中产生，并且与相应的证书一起被预先安装。此后，在安装过程中，该设备可以执行一个基于公钥的密钥协商协议（如互联网密钥交换，IKE[19]）引导根密钥。虽然听起来简单（使用已知技术），但使用这种方法有一些问题，包括需要一个可以处理十几亿设备的大型公钥基础设施（PKI）。

PKI 集硬件、软件、人、政策和程序为一体，需要创建、管理、分发、使用、存储和撤销数字证书[18]。此布置采用认证机构（CA）的方法把公钥与用户身份绑定，该绑定通过登记和发放过程建立。PKI 功能确立此绑定被称为注册机构（RA）。对于每个设备，设备的身份、它们的绑定、有效的条件和包含于公钥证书

中的其他属性，都是由 CA 签发的。CA 的主要作用是发布束缚于一个给定身份的密钥，这是通过使用 CA 自己的密钥来实现的，因此，设备的公钥的信任依赖于人们对 CA 的密钥有效性的信任。

8.4.2.1 数字证书和数字签名

数字证书认证公钥的所有权，这允许其他实体能够依靠于数字签名或私钥发表的声明，该私钥与被认证的公钥相对应。此模型中的信任关系是这样的，CA 是一个值得证书的所有者和证书的依赖方都信任的第三方，换句话说，证书是由 CA 构建的包含身份和公钥并把它们与数字签名结合起来的数字文件。该机构确保创建数字签名，并检查具有相应公钥的设备和拥有相应私钥的设备身份。拥有 CA 公钥的任何实体在提供的证书上可以认证 CA 的签名。基于此，（可信）CA 确保证书中的公钥属于身份在同一个证书中的实体。

全球公认的数字证书标准称为 X.509[18]，X.509 证书包含所签署的信息，因而，其可以保证信息是真实的和未经修改的。该信息可能包含序列号、有效期、发行者名称（是签发的 CA 的身份）、主题名称（是被认证的身份；可以是一个设备、运营商的认证服务器等）、隶属的公钥（被认证方的公钥），以及一个指示根 CA 与终端用户之间所允许的中间 CA 最大数目的路径长度字段，数字签名由签发 CA 的私钥产生。

8.4.2.2 使用证书进行 M2M 服务引导

在下面的章节中，对使用证书引导的不同可能的方法进行讨论，其中包括遵循 OMA DM（开放移动联盟设备管理）标准的方法。

1. OMA DM 规程

对于 OMA DM，DM 推动者一般使用 DM 服务器来实现将其存储管理对象（MO）使用 DM 协议转移到 DM 客户端，在 OMA DM 中，在以下三种情况中的任何一种情况之下，设备都将被引导：

● 在工厂的制造过程中。

● 拥有智能卡。

● 通过 DM 服务器，在设备和 DM 服务器之间进行初次握手之后，后者向设备发送根密钥。

在 DM 服务器向设备提供（推送）资料的情况下，在这一时间段内设备可以启动 DM 服务器的管理会话，采取下列步骤：

● DM 服务器和设备使用一个共享的密钥或身份验证信息的带外传送进行相互验证，共享的密钥可基于用户 PIN 或网络 PIN。证书也可用于此目的。

● DM 服务器采用推送机制发出引导信息，在启动引导之前，服务器必须知道设备的地址或其他一些机制用于和设备的通信。引导信息包含足够信息授权设备并发起与发出引导信息的 DM 服务器的会话，它是一种一次性传输的信息，而不是设

备和 DM 服务器当前会话的一部分。

在引导和设备的定期登记中，设备和 DM 服务器可以以各种方式进行相互认证，如：①传输层安全预共享密钥（TLS-PSK），其中预共享密钥是由制造商或 DM 服务器提供的，②有服务器证书的 TLS 和摘要式的客户端身份验证，客户端密码用于验证客户端身份，③有客户端和服务器证书的 TLS，客户端证书由制造商或 DM 服务器配置。

2. 使用证书引导

使用证书引导的潜在途径可能涉及下列方法（可包括在 OMA DM 范围之内）：

● 该设备由所有候选 M2M 提供商信任的 CA 预先配置一个证书，该 CA 可能是一个受信任的 CA，由实体运营维护与所有可能的服务提供商的业务关系，该 CA 还需要维持与所有设备制造商的业务关系，或被所有设备制造商所信任。该设备还预先配置一个或多个附属于服务提供商的 CA 的公钥。

● 在工厂制造时，该设备预先配置尽可能多的证书作为被所有候选服务提供商所信任的 CA 的总数目。在服务提供商拥有该 CA 的情况下，设备需要配置每个 CA 证书，该设备还预先配置一个或多个附属于服务提供商的 CA 的公钥。

● 在引导期间，设备由 CA 配置一个证书，这种 CA 必须是服务提供商所信任的（例如，后者拥有 CA），在这种情况下，设备需要被预先配置凭证，该凭证用于在接收证书之前（可能伴随着接收一个 RSA 私钥/公钥对，签发的 CA 提供了该种服务）的设备认证。

在上述情况下，每当证书被配置到该设备，就需要连接一个或多个受信认证机构，更具体地说，在制造商预先配置证书的情况下，在制造过程中需要配置设备，至少有尽可能多的证书作为现存的不同 M2M 服务提供商所信任的根 CA 的数目（假设制造商不是具有先验意识的特定服务提供商，该设备将被引导）。如果制造商拥有一个值得所有不同服务器提供商信赖的根 CA，那么所有服务器提供商需要信任所有的制造商；在这样的情况下，一个单一的证书（由制造商的 CA 签发）在工厂就可以被预先配置给设备。此外，设备还需要预先配置所有（可信的）CA 的公钥，其负责签发服务提供商证书。同样，如果证书的配置由服务提供商执行，后者则需要配置由可信的 CA 签发的证书（例如，服务提供商所拥有的）。显然，上述所有情况下，这样的证书配置将采用认证服务实体的所有潜在类型，也就是说，在 OMA DM 中不仅仅使用 DM 服务器。

证书的撤销基于证书撤销列表（CRL）查询或某些撤销协议，如在线证书状态协议（OCSP）[20]。CRL 查询需要额外的流量由设备或 M2M 服务提供商发起。由于要部署数十亿 M2M 设备，该查询被转化成跨越多个接入网络的更高的带宽占用（通常，增加网络资源占用），并因此提高了复杂性。CRL 数据库需要一直在线，以撤销相关的查询服务。由于 CRL 数据库只包含撤销证书的列表，它经常会返回一个不确定的结果：“证书的问题不在数据库中”。

基于以上的讨论，下面我们列出具体的问题，表明对于解决 M2M 引导问题，公钥加密方法可能不是很理想。

● 在蜂窝网络中，公钥的方法不属于现有的主要蜂窝标准，几乎所有的注册和相关链路层认证机制都使用对称密钥协议［3GPP、3GPP2 等］进行处理。通过无线的方式，使用任何公钥方法来引导密钥，这意味着设备在引导之前不能向移动网络注册。因此，只有在标准改变后才使用引导公钥方法，所以蜂窝 M2M 业务不会成为一种覆盖技术。

● 需要 PKI 管理证书（包括配置、维护和撤销）对于公钥方式的安全功能是至关重要的，在 M2M 背景下，任何公钥方式都限于引导每台设备的“一个对称密钥”，反过来又意味着交易成本会很高；也就是说，使用现有公钥方式和一个广泛的 PKI 证书管理，“每台设备的交易”是非常高的。为了长期使用公钥系统，PKI 的成本（尤其撤销）很高时，最终将摊销每个密钥的多个交易合理化。此外，对于复杂的生态系统，扩大现有的 PKI 来管理数十亿的密钥不是一个可扩展的操作任务。我们知道，M2M 设备可以是相当便宜的（例如，计量应用），因此，利用公钥方式引导安全协会将有意想不到的提高设备成本的效果。

● 另外，在公钥设置中的私钥必须安全地存储，由于 M2M 成本约束的性质，物理防篡改的安全性不能对证书和私钥提供长期保护。

● 而且，只有当多个节点与其他节点共享密钥时，公钥方式才具有吸引力，减少管理 $O(n)$ 密钥问题，而不是 $O(n^2)$ 密钥问题。我们处理涉及一台服务器上的多个设备共享一个安全协议的问题。

8.4.3　基于智能卡的解决方案

在 M2M 部署在蜂窝网络的背景下，使用智能卡（一般对于 GSM 系统或 UICC 使用 SIM 卡）是一个非常具有吸引力的选择。自 20 世纪 90 年代后期以来，蜂窝网络运营商已将 SIM 卡广泛应用于移动电话和其他与蜂窝基站相连接的移动设备。因此，在某些蜂窝 M2M 情况下，设备默认配备智能卡，这种卡可以为 M2M 服务或应用层提供所需要的密钥资料。

更具体地说，某些网络标准主要是由 3GPP 授权定义特定类型智能卡的使用，如带有 SIM 的 UICC 或 USM 应用，可用于连接到网络的任何设备。在这样的设置之下，M2M 设备授权智能卡的使用。智能卡包含一个预置的永久密钥，这是智能卡制造商的硬编码，并交付给网络运营商。该密钥可用于产生会话保护密钥，并被 M2M 服务层或应用层所使用，且各种技术都可以用于该密钥的导出，如通用引导架构（GBA）框架。

供较高层（服务、应用）使用的密钥生成和提供建议新密钥的接受者是信任智能卡所有者（密钥生成器）的实体，即蜂窝网络运营商。因此，如果生成的密

钥用于建立设备和 M2M 服务提供商之间的安全会话，M2M 服务提供商应与网络运营商具有信任关系。当网络运营商执行 M2M 服务提供商任务提供 M2M 设备时，该种方式尤为方便。同样，如果应用提供商信任网络运营商，网络运营商可以为应用提供商提供一个密钥用于建立端到端的应用层安全会话。再者，网络运营商可以向设备提供应用层服务（如操作应用服务器），因而 M2M 应用可使用存储在智能卡中的永久密钥及在运营商的安全密钥数据库中由协议萃取的密钥，显然，如果蜂窝网络运营商不被应用或服务提供商所信任，那么需要使用一种不依赖于智能卡的密钥配置的独立方法，除非这种方法可以网络运营商（如不受密钥用户信任的实体）无法获得的方式导出密钥。

智能卡不适合专门用于服务或应用层安全，这是因为智能卡固有地增加设备成本，且向智能卡中配置根密钥的问题常常脱离卡制造商而有可能是一个专有程序。当客户购买服务时，典型的方法是手动配置。但是，该方法在由数十亿设备组成的蜂窝 M2M 部署中不具有伸缩性，更重要的是，在蜂窝电话中使用智能卡的基本原则是启动可移接性的预约，即使终端用户使用任意设备并通过有效预约连接到网络而无需运营商介入。此功能在 M2M 环境中很少或根本就没有价值，实际上，任何可移动身份识别模块开启恶意终端用户在其他设备中使用这些卡并窃取服务的可能性（在这些情况下，M2M 应用服务由应用提供商所支付）。此外，当应用提供商与运营商之间进行切换时，需要更换智能卡。这可能需要更换数百万的智能卡，费用也可能会很昂贵，而且，这不能实现无人工干预。

8.4.4 基于预分配的对称密钥的方法

在 M2M 设备与 M2M 服务提供商两者都预分配相同的密钥的情况下，它们两者之间可实现相互认证，在每个设备注册期间，这可用于执行对称加密操作。在一个安全的环境内，该密钥可以在设备中永久地存储。在服务提供商看来，这样的密钥通常存储在一个安全的数据库中，其与认证服务器接口，如 HSS 或 AAA 服务器。

鉴于上面所讨论的关于 M2M 设备部署情景的多样性，不可能预先假设 M2M 服务提供商参与设备部署过程并分配给终端客户。此外，由于 M2M 设备的成本，在大多数情况下，设备没有配备可用于购买时手动配置密钥的用户界面。因此，对于预分配密钥解决方案，设备制造商负责执行以下两个方面的任务：

- 在出厂时，将密钥装入设备。通常，该密钥被存储于设备的安全环境之中。
- 向服务提供商随机（根据设备分布情况）分配相同的密钥，该分配可利用接口支持制造商的安全数据库的后台办公服务器。一般情况下，应用或服务提供商直接从制造商订阅和购买设备。

然而，可能会出现这样的情形，客户从零售商店购买设备，而需要满足不与运

营商或制造商保持任何业务关系。在这种情况下，制造商可能与任何其他 M2M 生态系统中的参与者不保持任何业务/信任关系。事实上，在这个例子中，制造商只需制造并向零售店销售 M2M 设备，甚至不直接向终端用户或应用提供商销售。由于缺乏涉及制造商的信任关系，其他参与者如设备用户/所有者和 M2M 服务提供商不能假设永不会发生涉及制造商的攻击行动（显式或隐式）。因此，制造商预分配的密钥一般不能作为永久密钥建立安全服务层会话。但该预分配的密钥可用于两个目的：①用作设备和服务提供商或设备和应用提供商之间的初始手动认证；②用于生成新的共享永久密钥，并不被非受信实体（如制造商）通过被动攻击以隐式或显式的方式获得的安全程序。

例如，在基于 CDMA 1x 的移动语音和窄带数据系统中，已规定一般的空中业务提供（OTASP）程序。OTASP 程序包括选择使用口令认证的密钥交换（PAK）[21] 配置一个长期密钥用于链路层的认证和机密。在 Differ-Hellman 密钥交换背景下，PAK 涉及密码的使用。此过程的关键步骤是在制造过程中在每个设备中配置个人密码，下面通过接入制造商以及 M2M 服务提供商或应用提供商的后台办公设施实现这些密码的离线共享。

8.4.5　基于身份加密的自引导协议

在 8.4.2 节中，我们讨论了在 M2M 中采用可能的 PKI 解决方案所带来的挑战。基于身份加密（IBM）的协议已被提议作为现有 PKI 公钥协议的替代方法，IBE 的思想是：用户设备的公钥是一个和该密钥有关的数学函数的身份[22]。因此，没有必要通过使用证书将实体身份与公钥相关联，由已知算法可知，公钥本质上来自于身份。注意，对 IBE，消息以 IBE 接收者的公钥进行加密。后者是可以使用相关的（其身份）仅为接收者可知的私钥对这些消息进行加密的唯一实体。这种私钥由 IBE 密钥生成功能（KGF）通过使用秘密的域发布，而公开的加密功能，通过使用由大量 PKI 加以管理的证书进行身份验证的要求已经过时了。IBE 加密信息的信息发送者所需的唯一加密资料是用于生成接收者公钥的一组公开的加密参数[3]。

根据该加密/解密过程依赖于某些椭圆曲线的固有特性及参与引导的实体预先已知的一组参数，IBE 基于椭圆曲线密码体制（ECC）的概念。IBE 可用于在两个实体之间建立共享密钥。在下文中，采用 IBE 的协议用于引导，并对在同一时间执行相互认证进行了讨论。称该协议为基于身份认证的密钥交换（IBAKE）[23]。在这样的情况之下可使用 IBAKE：由于缺乏业务/信任关系，第三方不能促进密钥引导。例如，在 M2M 运营商与设备制造商或接入网络运营商没有信任关系的情况下，IBAKE 可用于在 M2M 设备和 M2M 运营商的认证服务器之间引导一个永久共享密钥。IBAKE 协议包括两个参与者之间的三个信息交换，IBE 使用相应接收者的公钥对每条信息进行加密。由于信息是被 IBE 加密的，所以只有拟定的接收者才能

够对其进行解密。在三次握手之后，参与者相互认证并可以建立（引导）一个仅被它们俩所知的永久共享的密钥。

为了执行引导，需要给参与引导的实体分配一组参数。在下文中，我们主要考虑 M2M 设备和 M2M 服务提供商生成一个共享根密钥，然后将其安全地配置给身份认证服务器（例如，HSS 或 AAA 服务器）的情况。显然，不同利益相关者执行 M2M 运营商的任务，如蜂窝网络服务提供商，此时，可遵循该协议。

● 设备的临时 ID 和临时密码：在生产过程中，给设备分配一个公共身份（如，MAC_address@realm 的格式）以及一个临时密码。此密码用于 M2M 服务提供商（引导之前）通过某些被“推入”设备的资料进行临时认证。更具体地，在引导之前，设备需要确保由正确的 M2M 运营商来进行引导，同样，运营商需要验证将被引导的合法设备。使用临时密码使设备和 M2M 服务提供商之间进行相互认证，以获得到 M2M 运营商的初始连接资源。一旦已获得该连接，就要在设备与 M2M 运营商之间建立如下所述的永久订阅相关的凭据。

● 设备的相关 IBE 资料：在最初的设备激活和引导目的之下，设备需要分配 IBE 私钥。为此，设备使用“秘密域”及一组公开可用的加密参数与受信任的 KGF 联系，以生成一个 IBE 私钥。M2M 服务提供商的基础设施给设备和 KGF 之间的通信提供了便利。因此，为了设备与 KGF 的联系，在设备和 M2M 核心之间使用设备中预分配的临时密码首次进行认证。秘密域用于生成仅由 KGF 所知的私钥，因此，KGF 需在不承诺（单独或共谋）主动攻击方面成为一个值得信赖的实体。M2M 运营商从 KGF 到设备安全地分配生成的私钥，即使用适当的接口将生成的私钥放入设备中。注意，使用日期信息（包括于公钥之中）产生 IBE 私钥，因而这些密钥在使用期满时会自动撤销（无效）。由于这种自动失效功能，IBE 私钥在期满后就没有了用处；也不能被用于解密超出其发出时间帧的内容。该设备还配置了与 M2M 运营商相关的 KGF 的公共加密参数；且需与私钥配置结合产生该配置。注意，这里 KGF 并不需要在设备配置中存储任何私钥/公钥信息，因为这些密钥可在需求时重新产生。

● 运营商的 IBE 资料：运营商同样由相关信任的 KGF 配置一个 IBE 私钥/公钥对。运营商也配置设备的身份（从而公钥），以及该设备相关的 KGF 公共参数。注意，设备和运营商可能使用相同的 KGF，其也许是外部的或 M2M 服务提供商所拥有的。

8.4.5.1 IBAKE 协议的执行

一旦设备和运营商配置上述的加密资料并允许交换信息，它们就会继续执行 IBAKE 握手程序。如参考文献［23］所讲述，IBAKE 由设备和运营商之间的三个信息组成。该信息交换如图 8-1 所示，其描述如下：

● 设备选择一个随机数 x，用 ECC 计算 xP，其中 P 是椭圆曲线上的已知点。该设备使用运营商的 IBE 公钥加密 xP 并向运营商发送加密信息（MESSAGE_1）。如上面所提到的，只有运营商可以解密该信息。

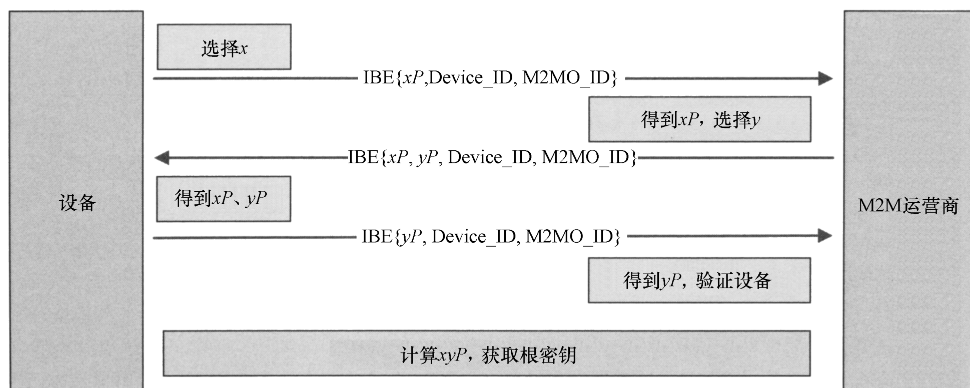


图 8-1　使用 IBAKE 的根密钥引导

● 运营商从设备接收并解密 MESSAGE_1，从而得到 xP。然后运营商产生一个随机数 y 并计算 yP。此外，运营商用设备的 IBE 公钥加密 xP、yP，并将信息（MESSAGE_2）发送至包含 IBE 加密的 xP 和 yP 的设备。

● 设备从运营商接收并使用 IBE 解密 MESSAGE_2，从而获得 xP、yP。如果接收到的 xP 值与从设备发送至 M2M 服务引导功能（MSBF）的初始消息相匹配，那么说明该设备已经认证运营商（特指参与引导的运营商基础设施中的服务实体），因为运营商是可以加密 MESSAGE_1 的唯一实体。随后，设备 IBE 加密 yP 并发回至运营商（MESSAGE_3）。运营商接收并解密 MESSAGE_3。如果获得的 yP 值与 MESSAGE_2 相匹配，那么说明运营商已经认证了设备。

如上所述，设备和运营商能进行相互认证，并拥有 xP 和 yP 值。并且，它们中的每一个都可以使用 ECC 功能计算 xyP，还可以通过使用公知 ECC 功能，用 xyP 来获得永久共享密钥。欧洲电信标准化协会（ETSI）M2M 功能体系架构规范提供了 IBAKE 协议如何用于 M2M 设备和网关的自动引导的详细信息。

8.4.5.2　IBAKE 的优势

前面提到的 IBE 方式有以下优势：

● 避免密钥托管点：所有协议交换中的在线步骤都使用 IBE 进行加密。因此，KGF 明显能够解密所有交换。但 KGF 不能计算出会话密钥，这是因为椭圆曲线 Diffe-Hellman 问题的难解性。换句话说，即使第三方获得 xP 和 yP，也很难计算出 xyP。因此，即使一个被动攻击者（将获得秘密域）破解了 KGF，也不能获得既定的（根）密钥。因此，仅在无法启动或促进主动攻击的情况下，需要信任 KGF。此外，虽然设备制造商已向设备预分配临时密码，制造商通过监听设备和运营商的通信可以获得设备的 IBE 私钥，但制造商不可能被动地获得根密钥；

● 引导期间设备和运营商的相互认证：正如上面所讲的，IBAKE 是一个相互

认证的协议；设备在收到 MESSAGE_2 后验证运营商的身份，而运营商在收到 MESSAGE_3 后验证设备的身份。

● 实现完整的前向和后向保密：因 x 和 y 是随机的，所以 xyP 永远是新的且与设备和运营商之间的任何过去或将来的会话无关。因而，一个新的 M2M 运营商无法获得旧的根密钥，而旧的 M2M 运营商无法获得未来的根密钥。

● KGF 的有效性：在 IBAKE 协议交换期间不接触 KGF，这极大地减少了外部实体的可用性要求。另外，如果运营商正期待执行设备引导，仅在此时，需要 KGF 在线。换句话说，如果 M2M 服务提供商拥有 KGF，在没有设备期望引导时，该提供商可设置 KGF 离线。

IBAKE 作为目前公布的一个互联网工程任务组以 MIKEY-IBAKE（多媒体互联网键控）的形式请求注释（RFC），并且考虑多种标准化组织，例如 ETSI 和 3GPP。

8.4.6 M2M 设备组的安全性

传统安全注册协议依赖于客户端（或设备）与服务器（或网络）的认证。例如，用户可以登录服务器，或移动设备可向网络登记。注册协议通常包括客户端/设备至服务器/网络的认证协议或相互认证协议。最近，人们已开始着眼于对整个会话过程进行保护（而不仅仅是接入），这些认证协议已经扩充到包括允许客户端/设备和服务器/网络一致达成一组密钥来确保整个会话的密钥协商。单向认证协议的例子包括挑战认证协议（CHAP）[1]、密码认证协议（PAP）[1]、基于三位元组 GSM 认证协议等，相互认证协议包括 3GPP 的认证和密钥协商（AKA）协议[2]，各种基于相互认证协议的可扩展认证协议（EAP），如 EAP-TLS[24]、EAP-GPSK（广义预共享密钥）等。

虽然上述的机制适用于 M2M 环境，但在数百或数千个设备需要被接入网络运营商、M2M 运营商或应用提供商在短时间之内进行认证的情况下，上述机制没有很好的伸缩性。因此，近来在各种标准化机构中已对设备组认证的概念进行了讨论。将拥有广阔视域的 M2M 设备组群纳入标准考虑的范围之内，也就是，不仅仅是出于安全目的，如在参考文献［25］所描述。设备根据特殊决策组合在一起，并知道它们所属的组。由可能的不同参与者执行该决策程序和开发决策的相关网络实体的功能，如共同或独立地工作的 M2M 运营商和接入网络运营商。

组认证时，一组 M2M 设备可以安全地使用单独的注册程序注册相同系统。这可以显著减少所需的与注册程序相关的信令，对于这一点，我们将在后面作详细的讨论。换句话说，没有必要与每个 M2M 设备建立单独的会话以达到单独认证每一个设备的目的。相反，属于特定组的设备成批进行认证，从而在很大程度上降低认证程序的复杂性和带宽要求。由组 ID 表示一组的 N 个设备，这是为相关组认证程序的所有网络实体所知的；相同的实体用于认证单个设备。这些实体也知道属于该组的所有设备的身份。这样信息可以查找表的形式存储在每个本地实体中。

为了提出一种组认证如何节省信令的思想，我们应考虑下面的例子。我们假设 N 个设备的部署和认证实体（认证器）在授权它们接入一个或多个服务之前需要对每一个设备进行认证。到目前为止，认证器需要建立一个单独的会话，并与每个设备交换固定数量的认证消息。因此，如果部署由 N 个设备组成，且若认证器和每个设备之间需要交换的消息数量为 k，则需要通过无线方式传送认证所有设备的消息总数为 $N \times k$。作为例子，我们假设 $N = 100000$，认证使用 AKA 协议[2,24]。按照此协议，认证器给客户端发送一个用户认证请求，其由一个随机质询（RAND）和一个认证令牌（AUTN）组成[4,7]；因此，在该例中 $k = 2$。其结果，是总共需要 200000 个单独的消息。整个过程结束时，N 个设备中的每一个设备将生成一个会话密钥，即在认证器和每个设备相互之间总共产生 100000 个会话密钥。注意，可能存在多个而不是一个认证器，每个认证器都认证一个不同类型的服务。在这种情况下，每个设备必须分别持有不同于每个认证器的认证程序（在这种情况下，可以使用“单点登录”的概念，其在设备中可以使用一组凭据并凭借各种不同的认证器进行认证）。在该环境下，一个可能的组认证解决方案将节省信令，而不是采用单独处理每个设备的方式，但是将所有 N 个设备作为一组，同时使用广播下行消息向它们发出质询。在这种方式中，只有一个（而不是 100000 个）消息必须被发送至所有 N 个设备。

虽然所有的设备都作为一组进行认证，但这种方法的密钥特征应确保由 M2M 设备的注册结果所产生的会话密钥是不相同的。该属性将允许每个 M2M 设备与服务器/网络进行安全通信而不破解组内的隐私。更具体地，应符合下列要求：

● 在独立设备认证情况下确保同等的安全强度。

● 为每个设备建立单独的、唯一的密钥，如安全的设备数据防止源自其他设备的（甚至是那些属于同一组的）可能的攻击。

● 使用数目减少的认证消息。单一认证程序的理想情况下，使用相同的带宽，与认证器进行尽可能多的信息交换。

该种程序的示例描述如下。

假设给属于一组的每个设备都分配了两个密钥，也就是唯一的独立密钥 Ku 和组密钥 Kg。再假设 AKA 认证协议用于执行交互 AKA。

在组认证中，认证器将请求专为组认证设计的 HSS 认证矢量。该矢量将包含随机质询（RAND）和网络认证令牌（AUTN）使用组密钥计算 Kg，同时也包含期望的认证结果$XRES_i$ 和一组会话密钥（CK | IK）$_i$ 使用每个设备的 Kg 和（Ku）$_i$ 的 XOR 对组中的每个设备进行单独计算。

认证器将向组中所有设备发送 RAND 和 AUTN 作为单独的广播消息。当计算一个特定的单一设备［CK，IK］$_i$ 时，组中每个设备将验证 AUTN 的有效性，并以单独的RES_i 进行响应。该响应被发回认证器验证并激活相应特定设备的会话密钥。

在这种交换中，对于组中的 100000 个设备仅有 100001 而不是 200000 个消息被交换，否则就属于常见的 AKA 交换例子中的情况。

虽然在写本书的时候不知道这样一个过程的细节，但组认证解决方案应用的预期利益是多方面的。

8.5 安全 M2M 和 MTC 通信的标准化工作

近年来，越来越多的关注聚焦于对 M2M 安全性的各个方面进行标准化。该关注符合标准化功能架构设置的平行工作。在下文中，我们讨论当前不同标准化组织的工作现状。

8.5.1 ETSI M2M 安全性

如第 2 章所述，ETSI M2M 标准化工作组的重点是设计 M2M 服务提供商的功能架构，认为 M2M 服务提供商是一个服务层实体，逻辑上位于接入层之上，并独立于（也可能联合）接入网络运营商及 M2M 应用提供商。

M2M 设备（或网关）和 ETSI M2M 服务功能之间建立安全数据会话的基础是存在密钥分级结构。

安全性源于设备内的安全位置（如设备信任的环境）以及 M2M 服务提供商处所的安全用户数据库中的一个永久存储的普通根密钥（K_{mr}）。该密钥被安全引导至设备和提供商，我们后面再作解释。根密钥用于网关和提供商之间的相互认证，以及产生临时注册的会话密钥（称为服务密钥（K_{mc}））。由于在设备与 M2M 服务提供商的服务引导期间，K_{mr}被引导至设备，只要设备属于相同的服务提供商，那么 K_{mr}可以永久地存储于该设备之中。在任何这种从属关系终止后，存储的根密钥将被丢弃。注意，一个设备可以同时从属于一个以上的 M2M 服务提供商。在这样的情况下，每个提供商的一个或多个根密钥被安全的存储于设备之中，该方式下，不同的提供商不知道对方的根密钥值。还要注意，根密钥被绑定到客户端身份；一个设备可掌握多个客户端身份，即使其属于单个服务提供商。此时，多个根密钥与每个客户端身份的单个密钥被再次存储并被设备所使用。

不论设备何时向 M2M 核心注册，K_{mr}密钥都用于设备（客户端身份位于设备之中）与 M2M 服务提供商的服务功能的相互认证。在相互认证成功后，设备和认证服务器使用已知的 KGF 使 K_{mr}产生 K_{mc}密钥。K_{mc}是对设备注册会话的持续时间有效的会话密钥。K_{mc}由安全认证服务器产生，并传送至网络安全能力（NSEC）在 M2M 核心的功能。事实上，NSEC 可能作为一个认证器参与相互认证过程。在这种情况下，NSEC 与 M2M 认证服务器（MAS）建立安全会话，其与存储用户根密钥的安全用户数据库相结合。设备的认证请求指向 NSEC，其依次请求并从 MAS 接收

认证资料。使用 TLS-PSK 或其他方法，K_{mc}可进一步用于设备/网关和 M2M 运营商之间的安全数据交换。

在 ETSI M2M 工作中，M2M 生态系统的复杂性是一个重要的考虑因素。需以这样一种方式对安全性进行标准化：满足生态系统中与潜在的信任关系相关的功能需求。基于此，ETSI M2M 明确区分关于安全性的两个高层次用例：

- M2M 服务提供商维持与其他参与者的业务关系，如接入网络运营商和设备制造商。
- M2M 服务提供商不信任生态系统中的其他参与者，因此服务层函数需要单独建立设备和 M2M 核心之间的安全关联。

在第一种情况下，M2M 服务提供商信任其他的利益相关者，如接入网络提供商和设备制造商。M2M 和接入网络提供商之间的现有信任关系表明可由接入网络提供商在永久性的基础上提供密钥资料，因为接入网络提供商支持该机制。例如，M2M 服务提供商可能会信任一个下属的移动网络运营商，其已经进行某些安全运营以保障从/到移动设备的通信量。在该信任环境中，接入网络运营商可从永久密钥中获得存储于 HSS/HLR（归属位置寄存器）和相应的 UICC 的安全密钥，并将其提供给 M2M 服务层用于建立安全服务层会话。GBA 方法是执行该密钥资料生成的方法之一[26]，其使用接入网络会话密钥来产生新密钥以供更高层使用。显然，接入网络运营商知道在服务层所使用的根密钥；但由于保持两个运营商之间的信任关系，所以这对 M2M 服务提供商不是一个难题。以类似的方式，设备制造商和 M2M 服务提供商之间的现有关系允许制造商向服务层提供用于建立安全关联的密钥。特别是，在制造过程中，制造商向设备预分配一个密钥并向一个或多个 M2M 服务提供商（这取决于设备将联合多少个这样的提供商）分配相同的密钥。由于制造商是一个值得信赖的实体，并以安全的方式向 M2M 服务提供商分配密钥，所以该密钥可能被用作根密钥。但在通常情况下，M2M 生态系统中不存在这样的信任关系，除非接入网络运营商或制造商直接提供 M2M 服务配置。

如果 M2M 服务提供商和其他实体之间不存在信任关系，M2M 服务提供商需要独立建立与关联设备的安全会话，在该方式下，不信任的实体不能被动地获得根密钥或会话密钥。换句话说，M2M 核心上的 M2M 设备和 M2M 服务功能之间应使用禁止获得根密钥或服务密钥的被动对抗性攻击的方法建立引导和安全数据会话，此方法涉及制造商和接入网络运营商。还要注意，这种方法需要考虑相关复杂的 M2M 生态系统及 M2M 设备的有限功能。该方法用于根密钥引导的可能例子在 ETSI M2M 标准中已经出现，并可以在参考文献［27］中找到。

8.5.2　3GPP 安全性相关的机器类通信网络性能提升

规范机器类通信（MTC）已经获得了来自 3GPP 的许多关注。3GPP 安全组

（SA3），已由组需求和网络架构组（分别为SA1和SA2）引导面向设计和规范化与MTC网络性能提升相关的安全程序。由于3GPP主要针对专有运营，包括部署的3GPP网络、架构，因而支持M2M通信的安全与现有的3GPP网络设计相关。

MTC安全的主要要求是与非MTC通信相比，MTC优化不能降低安全性。由于这种广泛的要求，SA3的任务是设计安全解决方案以保护MTC特性的功能，并由SA2进行定义和规范。这些特性与组通信、时间控制、低流动性、监控、IP地址、小的数据传输、设备触发、信令拥塞控制等相关。SA2提供了每个MTC特性设计的最新草案版本。SA3的任务是确定已规范化的安全对策是否受新设计的影响，并进一步消除已识别出的安全设计的缺陷。

参考文献

1. Mizikovsky, S., Wang, Z., and Zhu, H. (2007) CDMA 1x EV-DO security. *Bell Labs Technical Journal*, 11 (4), 291–305.
2. 3GPP TS 33.102. Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 9, 2009).
3. European Telecommunications Standards Institute (1997) GSM Technical Specification GSM 03.20 (ETS 300 534): Digital Cellular Telecommunication System (Phase 2); Security Related Network Functions, August 1997.
4. Aboba, B. and Simon, D. (1999) PPP EAP TLS Authentication Protocol. RFC 2716.
5. Cox, R., Grosse, E., and Pike, R. (2002) Security in plan 9. USENIX Security Symposium, 2002.
6. 3GPP TS 33.401. Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security Architecture (Release 9, 2009).
7. Gallagher, M.D. and Snyder, R.A. (1997) *Mobile Telecommunications Networking with IS-41*, McGraw-Hill, ISBN: 0-07-063313-2.
8. Handley, B. (2000) Resource-efficient anonymous group authentication, *Financial Cryptography, 4th International Conference FC 2000 Anguilla*, British West Indies, Springer-Verlag.
9. Gohil, S. and Fleming, S. (2004) Attacks on Homage Anonymous Group Authentication Protocol. Technical Report OUCS-2004-16, Department of Computer Science, University of Otago.
10. Jaulmes, E. and Poupard, G. (2002) *Financial Cryptography 2001,* Lecture Notes in Computer Science, Vol. 2339, Springer-Verlag, pp. 106–116.
11. Hanaoka, G., Shikata, J., Hanaoka, Y., and Imai, H. (2005) *Unconditionally Secure Anonymous Encryption and Group Authentication*, Oxford University Press, December 2005.
12. Martucci, L.A., Carvalho, T.C.M.B., and Ruggiero, W.V. (2004) A lightweight distributed group authentication mechanism. Proceedings of the 4th International Network Conference, INC, July 2004.
13. Kent, S. (2005) Security Architecture for the Internet Protocol. RFC 2401.
14. Teofili, S., Mascolo, M.D., Bianchi, G., Salsano, S., and Zugenmaier, A. (2008) User plane security alternatives in the 3G evolved Multimedia Broadcast Multicast Service (e-MBMS). *Security and Communication Networks*, 1 (6), 473–485.
15. Arkko, J. and Haverinen, H. (2006) Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA).
16. Feng, Z., Ning, J., Broustis, I., Pelechrinis, K., Krishnamurthy, S.V., and Faloutsos, M. (2011) Coping with packet replay attacks in wireless networks. IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2011.
17. Droms, R. (1997) Dynamic Host Configuration Protocol. RFC 2131.
18. Cooper, M., Dzambasow, Y., Hesse, P., Joseph, S., and Nicholas, R. Internet X.509 Public Key Infrastructure: Certification Path Building. RFC 4158.

19. IETF RFC 4306. Internet Key Exchange Protocol.
20. Myers, M., Ankney, R., Malpani, A., Galperin, S., and Adams, C. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. RFC 2560.
21. Brusilovsky, A., Faynberg, I., Zeltsan, Z., and Patel, S. Password Authenticated Key (PAK) Diffie-Hellman Exchange. RFC 5683.
22. Boyen, X. and Martin, L. (2006) Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems. RFC 5091.
23. Cakulev, V. and Sundaram, G. (2011) IBAKE: Identity Based Authenticated Key Agreement, Internet draft, http://tools.ietf.org/html/draft-cakulev-ibake-03.
24. Simon, D., Aboba, B., and Hurst, R. (2008) The EAP-TLS Authentication Protocol. RFC 5216.
25. 3GPP TR 23.888 System improvements for Machine-Type Communications (MTC) (to be published in 2012).
26. 3GPP TS 33.220. Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (2004).
27. ETSI TS 102 690. Machine-To-Machine Communications (M2M); Functional Architecture. (Release 1, 2010).

第 9 章　M2M 终端和模块

Gustav Vos
司亚乐无线通讯公司，不列颠哥伦比亚省，加拿大

本章重点讨论 M2M 的模块、特点，以及它所提供的服务。讨论这些内容之前，首先要对 M2M 模块提供一个明确的定义。一个 M2M 模块不同于 M2M 终端，一个 M2M 终端分解成两个逻辑组件。第一个是终端的应用部分，它为 M2M 应用提供了具体的硬件和软件部分。例如，在一个销售终端点，应用部分应该是键盘、LCD 以及与应用层软件相关联的打印机。M2M 终端的第二个逻辑组件的是 M2M 模块，它主要负责提供连接服务。应用部分有时也简单地称为 M2M 模块的“主机”。M2M 终端的应用部分和 M2M 应用高度相关，这部分内容将在本系列丛书的第二本书《物联网：关键应用和协议》中详细介绍。尽管 M2M 模块存在于有线和无线变量中（在本章后面介绍），但是我们在本章中更多介绍的是无线 M2M 模块，因为 M2M 模块的开发大部分使用的是无线网络。

9.1　M2M 模块分类

随着 M2M 应用所解决的问题高度多样化，毫无疑问 M2M 模块也有一个同样多样化的分类。以下部分提供了一种不同 M2M 模块的分类方法并提出了一些关键分类。但这些分类不是垂直的，这样，M2M 可以有更多的分类方法。这些分类还可以帮助应用开发人员来确定哪种类型的 M2M 模块对于一个正在开发的 M2M 应用是最适合的。

9.1.1　接入技术

9.1.1.1　无线和有线

第一个也是最简单的 M2M 模块分类方法是根据它所支持的接入技术类型来分类。有两种主要的接入技术类型：无线和有线。有线接入技术需要与电缆物理连接，比如电话线（例如 RJ11）或者有线电视公司的同轴电缆（例如 RG-6）。M2M 中一些更为流行的有线接入技术有电力线通信（PLC）（连接交流电源）、以太网（RJ-45）和 XDSL。无线接入技术在 M2M 中不常见，主要是因为不支持机动性、铺设新的电缆（PLC 除外）所引起的高的基础设施成本、维护比较复杂。另一方

面，无线或无线接入技术（RAT）不需要物理连接，它使用无线电波来传递信息。RAT 通常用于 M2M 应用，所以我们在以下部分主要介绍无线 M2M 模块。

9.1.1.2　无线链路距离

分类无线接入技术的一种方法是通过一个无线连接可以维持的距离进行分类，可分为无线个人局域网（WPAN）、无线局域网（WLAN）和无线广域网（WWAN）。如图 9-1 所示。

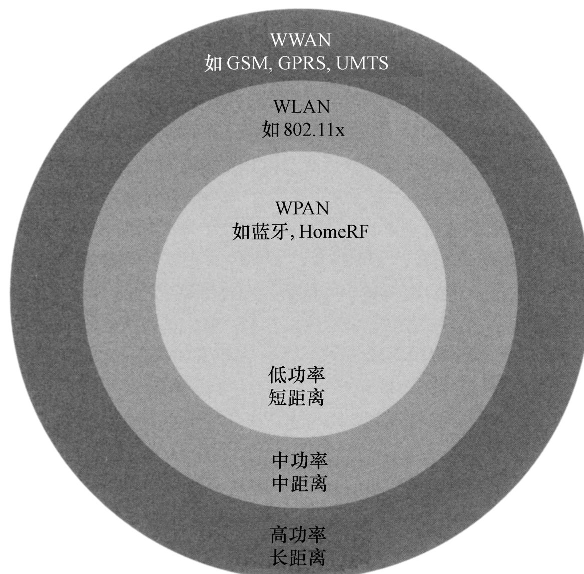


图 9-1　WPAN、WLAN 和 WWAN

一般来说，一个个人局域网链路覆盖范围低于 10m，所涵盖的技术如蓝牙、无线个域网（ZigBee）、超宽带，有时有红外线。无线局域网覆盖范围不超过 30m，这是一个可以覆盖一座办公楼的距离。最流行的无线局域网技术是 802.11（或 WiFi）。一个无线广域网可以覆盖很长的距离，它对于 M2M 模块是一个很流行的接入技术，因此本章余下的部分我们主要集中于此。无线广域网 M2M 模块是唯一的支持完整的流动性的无线接入方法，在 M2M 应用中很受欢迎。无线广域网可以使用以下的接入方案进行进一步分类：

- 频分复用（FDMA），例如 AMPS。
- 时分复用（TDMA），例如 GSM。
- 码分复用（CDMA），例如 UMTS。
- 正交频分复用（OFDMA），例如 LTE。

不同的无线广域网技术在吞吐量和延迟方面提供了不同级别的性能。是否使用某一种特定的无线广域网技术具体取决于应用的吞吐量和延迟需求。

9.1.1.3 代

无线广域网进一步的分类方法是通过“代”来进行的。就像其他所有的技术一样，无线广域网也在不断发展着。有时是改进增量，但是大多数时候更好的是根据代来改进，例如2G或3G。虽然市场以及广告部并不总是与国际电信联盟定义保持一致，这可能导致术语上的不协调，但是国际电信联盟已经规定了3G和4G的最低性能规格。在本章中会应用到以下分类：

- 1G（1代）包含技术有AMPS、TACS和NTACS。
- 2G包含技术有IS-136、GSM和1xRTT的大多数商业部署。
- 3G包含UMTS、TD-SCDMA和EVDO。
- 3.5G包含技术有HSPA（高速分组接入）等。
- 4G包含UMB（超移动宽带）、WiMAX（802.16e）和LTE。

尽管市场指出LTE和WiMAX（802.16e）为4G，严格地说，也没有满足国际电信联盟对4G性能的需求。2010年11月，国际电信联盟提出先进的LTE和WiMAX 802.16m接入技术作为4G技术，但是市场是否接受这个技术还不确定，可能是4.5G或5G。初步迹象表明，4.5G技术最早可能到2013年商业化。

9.1.1.4 2G主导地位

尽管无线广域网电话的零售渠道主要是新型的接入技术（例如3G），但M2M模块不遵循这种趋势，因为2012年无线广域网中大部分M2M模块主要部署在2G。尽管现在市场趋势逐渐向3G和4G模块演化，但超过2G模块还是需要很长时间，部分原因是因为M2M应用的生命周期长。例如，汽车或其他实用计量工具可能有十年的开发时间。2G M2M模块在2012年仍然被使用的原因主要包括：

- 2G能明显降低模块成本。然而，2G和2G+3G的模块成本差异正在迅速降低。
- 2G模块更成熟，也就是说，它更可靠、低耗能，而且有更多的特点和服务（参考下面的服务部分）。
- 2G覆盖率很好。因为大部分2G最初是在低频带上开发的（蜂窝GSM频带在800~900MHz），3G在更高的频带上（1800MHz DCS和1900MHz PCS）。2 G有一个天然优势，它有更好的覆盖范围，尤其是对室内穿透。
- 2G已经足够好了，因为模块可以在2G模型中而且是很有可能在农村和室内操作（参考前文），而且M2M应用需要2G的吞吐量和时延。
- 3G甚至4G中M2M模块缓慢变化的趋势可能会由MNO（移动网络运营商）或电信监管机构而引起非常迅速地加速。例如MNO可能禁止新的2G模块出现在他们的网络中，因为他们计划重新分配2G频谱来开发更多的3G或4G技术，甚至计划完全解除2G网络。另一种可能性是，如果MNO在他们的3G和4G网络收取更少的服务费用，这样新技术的总成本也不高。MNO也可能增加3G和4G设备来

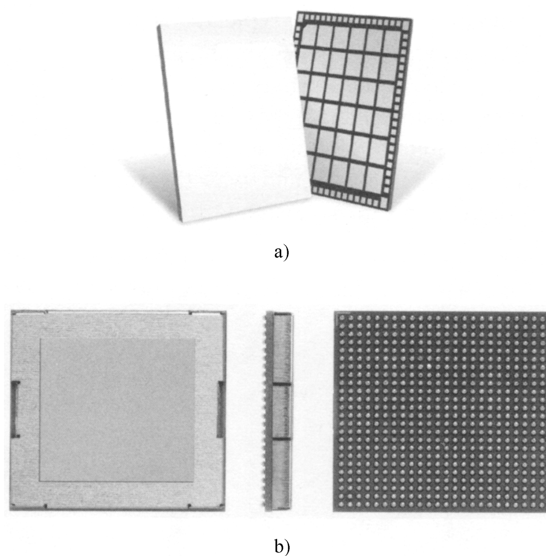
弥补和 2G 网络的差别。至于 MNO 决定何时解除 2G 网络系统也是很复杂的，有很多变化。有地理位置敏感上的变化，比如说频谱和标准制订，因此可以推断 2G 频谱的重新分配和 2G 系统的解除都高度依赖于地理位置。

9.1.2　物理形式因素

物理形式因素是 M2M 模块的另一种分类方法。形式因素与 M2M 应用开发者所需要的集成的级别很有关系。具体来说，形式因素越小，M2M 应用开发商要求的集成效果就越高。形式因素也与 M2M 模块可使用的硬件接口有关，较大的形式因素通常有更多可选择的物理接口。

9.1.2.1　焊接模块

第一个形式因素类别就是焊接模块。根据定义，这个模块没有连接器，它只有焊垫或焊料球用来和 M2M 终端的 PCB 进行焊接。焊垫用于线栅阵列（LGA）接口，焊料球用于球栅阵列（BGA）接口。使用 LGA 和 BGA 接口的 M2M 商用实例如图 9-2 所示。



a)

b)

图 9-2　（图来自 Sierra Wireless）
a）LGA　b）BGA

一般来说，焊接模块是形式因素中可用的最小的模块，在大多数情况下，这种尺寸的减小是通过使用一个多芯片模块（MCM）来实现的，它是一个集成电路（IC）包，在包里多个半导体芯片被打包到一起，以促进它们作为一个单集成电路的应用。由于这项技术既费时又需要更高的研发成本，因此越来越少的 M2M 模块供应商支持这种类型的形式因素，比较新兴的 WWAN 技术（例如 4G）也就稍微

落后于其他形式因素，比如说 PCI Express 迷你卡。焊接模块的大小在 25mm × 30mm 左右。即使受大小和 I/O 引脚的约束，这些模块仍然经常支持许多 I/O 接口，比如说 USB、I^2C、SPI 总线、UART 和 GPIO，这些通常为 M2M 应用开发商提供了足够的灵活性。所有的 I/O 都是通过表面贴装技术（SMT）封装，除了很少情况下需要提供一个天线连接。除了面积小，这种形式因素还有灵活性好的优点，因为它不需要连接器，而连接器受振动影响变得不可靠。因为热能可以很容易地从 M2M 模块中转出并转入到更大的 PCB 中，这种形式因素有着更优越的散热特性，使得它更适合于高温环境。由于存在散热和可靠性强的优势，这种焊接形式因素成为汽车应用的一个合适的选择，但是只有很少的 M2M 模块应用于汽车模块，因为需要大型认证负担，比如说 ISO TS-16949 生产规则。然而，仍有一些不乐观的下降趋势，主要的缺点就是它需要更多的来自 M2M 应用开发商的集成成本和代价。尽管集成代价越来越大，而且是专门定制的，独立的模块认证规则（参见认证部分）仍然适用，所以认证的努力和成本与使用其他模块形式因素一样。其他的缺点包括缺乏标准，所以客户容易锁定一个供应商，维护就更加困难，因为要更换一个有问题的 M2M 模块并不容易，而且升级也存在很多问题，例如，一种新的接入技术。

9.1.2.2 PCI Express 迷你卡

PCI Express 迷你卡形式因素，常被简单地称为迷你卡形式因素，它是由外围部件互连特殊利益团体（PCI-SIG）开发，并在 2003 年 6 月最终通过。尽管这种迷你卡标准支持两种主机接口连接——PCI 串行总线和 USB 2.0 连接，但是大部分 M2M 模块开发商只支持 USB 2.0 连接。PCI 串行总线的迷你卡的物理尺寸指定是 30mm×50.95mm，最大厚度是 5mm。PCI-SIG 还规定了一个指定尺寸为 30mm × 26.8mm 的半身长的卡（见图 9-3，商用中全身和半身大小尺寸的迷你卡）。

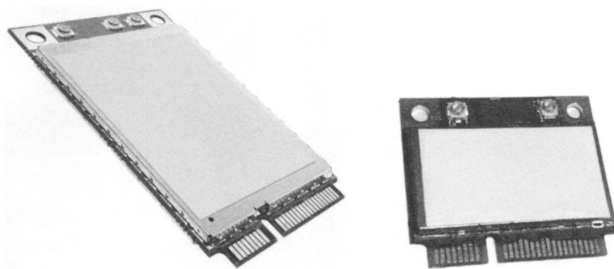


图 9-3 全身和半身大小尺寸的迷你卡（图来自 Sierra Wireless）

除了天线连接器，所有的 I/O 接口都是通过 52 引脚系统连接器来实现。虽然 PCI-SIG 没有明确定义，但天线连接器的位置通常在 PCI-SIG 所定义的 I/O 连接区域与系统连接器相对的一面。

这种迷你卡标准最初是用于笔记本电脑和个人电脑，但现在已经扩展到多种类型的 M2M 终端。大多数 M2M 模块供应商都提供这种形式因素，而且一般具有最完整和领先的接入技术，是第一种支持 4G 技术的形式因素。由于系统连接器是为易插入而设计，所以对于这种形式因素来说因故障而代换或技术升级不再是问题。

M2M 应用开发者所需要的集成程度低于焊接形式因素，但它仍包含机械外壳、电源供应、智能卡阅读器、天线、认证和软件驱动程序。虽然物理形式因素是为迷你卡标准化，但是与主机的软件接口却没有。这就暗示了供应商之间的交互性并不真正存在，因为 M2M 应用开发商在转换时仍然需要重新集成一个新的软件接口。这就降低了标准化为 M2M 应用开发商提供的优势。

9.1.2.3　高度集成

高度集成的 M2M 模块通常归类为有商用外壳和一个标准化的主机接口，比如 USB、RS232 或 RJ45 连接器（见图 9-4，高度集成模块的商用例子）。

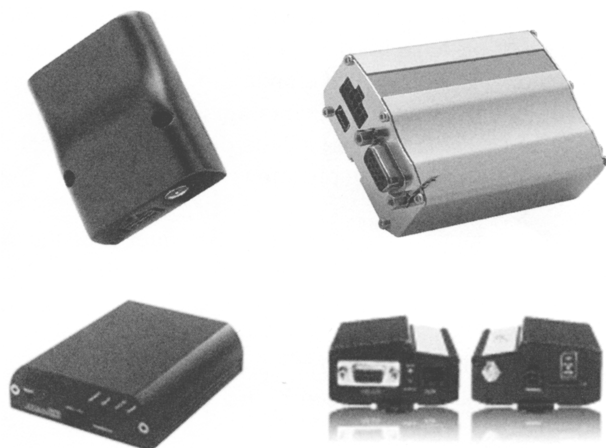


图 9-4　高度集成 M2M 模块的商用例子（图来自 Sierra Wireless）

高度集成的 M2M 模块的大小没有标准，但它却是最大的形式因素。使用高度集成模块的关键优势在于 M2M 应用开发商有更少的集成，几乎没有做认证测试（见 9.6 节关于认证的部分）。这些类型的 M2M 模块通常被称为网关终端，因为它们包括网关服务功能，从而允许支持多个主机，这也是 M2M 应用很大的优势。

9.1.2.4　专有

最后一种形式因素分类是专有形式因素，对于上面提到的其他形式因素，它是一种一般的非正交的形式因素。几乎所有的供应商在他们的投资中有一些专有 M2M 模块（见图 9-5，专有 M2M 模块的商用例子）。

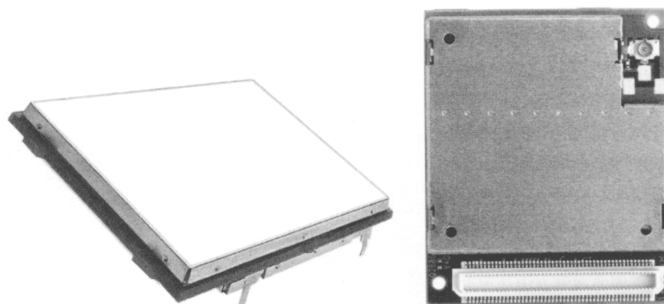


图 9-5 专有 M2M 模块的商用例子（图来自 Sierra Wireless）

这里的优势是高度多样化，但是一般来说，由于 M2M 模块供应商在任何情况下都不受约束，他们可以生产出一个更小、成本更低、更可靠、有更好的散热性或者是更专门的特定 M2M 应用的模块。

9.2 硬件接口

考虑到 M2M 应用的多元化的特点，M2M 模块供应商试图向开发人员提供几种接口选择。本节主要描述大部分可用的硬件接口。

9.2.1 电源接口

虽然一个电源接口受制于所有模块，但是所支持的电源电压范围在 3.0 ~4.5V 之间。一些模块可能需要更多的电压来供睡眠模式、高性能的功率放大器或实时时钟来使用。

9.2.2 通用串行总线（USB）接口

对于那些高速率的接入技术（比如说 3G 及其以上)，USB 接口是较好的通信接口。它还可用于调试，但许多模块需要提供不止一个 USB 接口来用于调试。大多数遗留的 M2M 模块只支持最高速率为 12Mbit/s 的 USB 标准，但由于最近接入技术无线空中（OTA）速度的增加，M2M 模块供应商也要支持高速（480Mbit/s）的 USB 标准。M2M 应用中 USB 在线功能的有限性导致很少有供应商愿意提供这种功能。

虽然 M2M 模块支持标准 USB 接口，但这种接口所使用的方法是已经配置好的。比如说，端点和通过端点的数据的增值是非标准化的。因此，每一个 M2M 模块供应商需要专业定制的 USB 驱动。如果主机使用有一个主流的操作系统（例如 Windows、Linux、iOS、Android、WinCE)，M2M 模块供应商通常愿意提供这些驱动。

9.2.3　通用异步接收器/发送器（UART）接口

UART 接口是一个非常普遍的主机接口，尽管它正慢慢地被 USB 接口所取代。UART 接口主要用于商业或调试功能。模块支持的波特率是 1200 ~ 115200bit/s，但最终这不应该成为通信中一个瓶颈，它应该大于 M2M 模块所支持的接入技术所提供的最大在线数据速率。由于一个 UART 本身不支持数据和控制信号通过一个接口多路复用，所以通常会使用两个 UART：一个用于用户平台，另外一个用于控制信号。

9.2.4　天线接口

每一个无线 M2M 模块都必须有一个天线接口，它可以是一个天线垫，也可以是一个天线连接器。天线的设计和它的位置通常与 M2M 应用开发商息息相关，这样在性能、大小、接口和形式因素方面就可以做出正确的取舍。很多新兴的接入技术需要更多的天线来完成接收多样性和多输入多输出信号处理。第二种天线通常用于接收（而不是传输），因此其设计参数的权衡是不一样的。如果模块支持嵌入式 GPS，这将需要一个天线接口。然而，这并不意味着需要另一种物理连接器。因为 GPS 天线可以通过以下几种方式实施：

- 与原来的无线广域网天线共享。
- 与二级或多样性 WWAN 天线共享。
- 单独的天线连接器。

9.2.5　通用集成电路卡（UICC）接口

该模块将用于 GSM 进化系统（例如，GSM、UMTS 或 LTE）或一些 CDMA 系统，一般都有一个通用的 UICC 标准（ISO 7816-3-based）。只有电气接口是 M2M 模块提供（除了高度集成的 M2M 模块），所以 UICC 读卡器的集成度和位置是由开发商提供。这就允许 M2M 开发商为 UICC 选择易进入、不可替换的优越位置，或者 UICC 不容易被盗的安全位置。

一些供应商把 UICC 嵌入到 M2M 模块中。这种嵌入式的 UICC 可能有一个专用形式因素或者一个标准化的形式因素，比如欧洲电信标准化协会智能卡平台组在 ETSI TS 102 671 中规定的 MFF2。由于这种嵌入式的 UICC 不能重复编程或替换，所以大多数供应商建议用一个额外的 UICC 读卡器来实现更高的灵活性。如果将来 UICC 可重复编程，那么 M2M 模块需要支持 UICC 接口，而且 M2M 应用开发商所用的集成 UICC 读卡器也将被淘汰。

9.2.6 通用输入输出（GPIO）接口

GPIO 接口主要用于控制外部外设和接收数字输入。

9.2.7 串行外围接口（SPI）

串行外围接口总线，也称为“四线”串行总线，是一个同步串行数据链接，在全双工模式下运行的，设备被配置为主动或者辅助。这种接口支持最高 70MHz 的时钟频率。这是一个通用的接口，可以用来控制许多周边设备，但常用于控制外部显示设备。

9.2.8 I^2C 接口

与 SPI 接口类似，但较慢，这种 I^2C 接口也称为“二线”接口，是一个同步串行数据链接了一个多控制总线。I^2C 总线传输速率高达 400kbit/s。这是一个通用的接口，可以用来控制众多的外围设备，但通常用于控制外部显示器、读传感器或存储外设。

9.2.9 模-数转换器（ADC）接口

M2M 模块中的模-数转换器接口主要用来对外部传感器提供的外部电压采样。

9.2.10 脉码调制（PCM）接口

M2M 模块中的脉码调制接口用于数字音频传输，通常是语音。

9.2.11 脉宽调制（PWM）接口

脉宽调制接口为 M2M 模块提供伪模拟输出，主要用于控制灯、按钮和模拟电源输出，通用性很强。

9.2.12 模拟音频接口

支持语音服务的 M2M 模块中将至少有一个模拟音频接口，包括一个音频输入和一个音频输出接口。

9.3 温度和耐久性

大部分模块提供一个工作温度范围是 -30 ~ +70℃，符合大部分工业应用，但汽车、计量和一些其他工业应用要求更高的操作范围 -40 ~ +85℃。热冲击循环是另一个重要参数，模块供应商通常在一些模块提供多达 1000 次热冲击的循环。

9.4　服务

M2M 模块提供的预先集成和支持的服务通常是最重要的，开发商需要考虑何时选择一个 M2M 模块会影响成本、上市时间和可靠性。应用设计和开发成本占总所有成本（TCO）很大的比例。全球移动通信协会（GSMA）发表了一篇名为“嵌入式模块指南”的文章，指出总体拥有成本中只有 3% ~7% 与 M2M 模块成本有关，而 20% ~40% 与非经常工程成本有关，也就是说，大范围是由 M2M 应用的多样性引起。这些数据也被一个类似发现所支持，是在 2010 年 11 月 GSMA 委托发布的一份报告中，Mason 发表在“TCO 用于嵌入式移动设备”。以下部分描述一些 M2M 模块中能提供的最常见的服务。

9.4.1　应用执行环境

大部分的主要模块供应商支持 M2M 模块中的应用执行环境。在这种情况下，M2M 模块和主机之间的区别变得模糊，只有在逻辑上是最好的。应用执行环境通常只适用于如 2G 和 3G 这样更成熟的接入技术（尚未应用在 LTE 模块中），该特性需要 M2M 模块供应商更多的研发。为了创建应用执行环境，M2M 模块可能有一个专用的应用处理器集成到 M2M 模块或可能使用某种形式的虚拟化的处理器来共享协议功能。M2M 模块供应商已竭尽全力使用行业规范和灵活性，尽可能使 M2M 应用开发人员更好的熟悉开发环境，但有可能是一些最初和专业培训需要的。这里列出更多既定 M2M 模块支持的许多特性：

- 标准化的集成开发环境，比如 Eclipse。
- 编程语言的选择，比如 JAVA，LUA，C + +，C。
- 实时编程，比如小于 1ms 的延迟到外部中断。
- 预先的多任务处理，比如优先任务。
- 事件驱动编程设计，比如“回调”功能处理。
- 空中（OTA）应用下载/更新和调试。
- 存储器接入保护（防止一个从崩溃终端的恶意存储器接入）。
- 调试工具，比如终端模拟器，远程跟踪监测。

适应于 M2M 应用处理电源的数量随着 M2M 模块供应商而变化，但是通常都不超过 50 个 MIPS，足以运行很多 M2M 应用，比如计量、销售点、汽车诊断或车队管理。使用支持应用执行环境的 M2M 模块对物料清单（BOM）存储和 PCB 的简化具有重要意义，因为它可以消除特定应用 CPU 的需求和相关的外围硬件，例如，电源管理、RAM 或者 Flash。因为应用执行环境包含一个操作系统和开发工具，软件许可成本也会减少。

TTM 和开发成本也会减少，因为许多预制和预集成的服务，比如，TCP/IP、SMTP（电子邮件）、FTP 和 HTTP 都是通用的。在 2011 年，应用执行环境虽然只在 4G 模块中使用，但鉴于利益方面，就 BOM、TTM、开发、许可和维护成本而言，该特性也将迅速迁移到 M2M 模块成为最新的接入技术。

9.4.2 连接性服务

假定 M2M 模块提供基本信息包交换连接，但它也很容易找到一个涉及 WWAN 连接性的 M2M 模块支持附加的服务。下面的部分描述了一些 M2M 模块供应商可能提供额外的连接服务。

9.4.2.1 SMS 唤醒服务

虽然理论上分组交换（PS）WWAN 系统应该提供 M2M 模块接通连接，以便它可以从一个 M2M 应用服务器接收移动终止或推送数据，但是实际上这个服务并不是在商业 WWAN 部署系统中容易获得的。导致这种不足的一些原因包括有限 WWAN 公共数据网络网关，如网关 GPRS 支持节点（GGSN）能力、公共 IPv4 地址瘫痪、网络地址转换器的使用和额外的 M2M 模块功率消耗（比如一直运行中）。因此在实践中，M2M 模块是被迫地运行在一个伪电路交换（CS）方式中，此处的 M2M 模块总是连接在 CS 域的 WWAN 系统而仅间歇性地连接到 PS 域。由于一直连接到 CS 域，这就允许 M2M 模块不断接收 SMS。如果一个 M2M 应用有数据要发送给 M2M 模块，M2M 应用将首先发送一个特殊的唤醒 SMS 到 M2M 模块，收到后，M2M 模块将解码和启动一个 PS 域连接，这样 M2M 应用就可以将数据推送。大多数 M2M 模块中这个 SMS 唤醒服务通常是预定义的，通常使用预先集成到可用的应用程序编程接口（API）。将来，4G 系统将有可能能够用有效的成本提供一种可伸缩的不间断 PS 连接，但 SMS 唤醒机制是根深蒂固在许多应用及如设备管理（DM）和 SIM 管理等服务中。因此，这种 SMS 唤醒方法可能仍被用于 4G 系统中，允许应用层向后兼容性。

9.4.2.2 分组交换服务

虽然 M2M 模块中主要是提供一个可靠的 PS 数据连接，但在 IP 层有相当多的复杂的协议都由 M2M 应用开发人员处理。尽管 M2M 应用后端服务器与 M2M 终端经常使用标准化的传输和通信应用协议，但这些协议的集成度和/或开发仍需 M2M 应用开发人员付出漫长和昂贵的代价。出于这个原因，成熟的 M2M 模块供应商提供预先集成的服务插件，最常用的有基于分组的协议，比较节约成本。一些更常见的可用的 PS 服务插件包括：

- TCP/IP 栈。
- SMTP。
- POP——邮局协议（因特网电子邮件协议）。

- FTP。
- HTTP（万维网协议）。
- XML——可扩展标记语言。
- SSL——加密套接字协议层。

当 M2M 模块也提供了一个应用执行环境的时候这些类型的服务是更常见的。因 M2M 模块供应商是在其自己的环境中的专家，这些插件的表现往往有可能超过 M2M 应用开发人员预期达到的目标。

9.4.2.3　电路交换数据

在 WWAN 系统提供分组交换数据服务之前，电路交换数据业务的数据连接是唯一可选的。一个电路交换数据连接在发送任何数据之前需要呼叫建立程序，这样专用资源的分配和释放直到一个呼叫拆卸过程开始为止。尽管大多数模块支持某种形式的电路交换数据，但它很少在商业上使用，因为电路交换数据有很多弊端。如果通信链路中有缺口，那么在电路交换数据中分配的专用资源不能在这个空闲时间被重用，这是非常低效的。对于电路交换数据的调用，WWAN 系统运营商可能还必须为公共交换电话系统提供一个调制解调器，这使得服务昂贵而且没有可伸缩性。M2M 后端应用可能还必须提供一组调制解调器。移动终端数据并不支持电路交换数据但支持 SMS 唤醒服务，如在上述描述中启动一个电路交换数据调用。然而，电路交换数据的优势是拥有一个常数延迟，例如，没有抖动。

9.4.2.4　语音/传真

虽然语音和传真在一些 M2M 模块中可适用，但这与电路交换数据类似，是一个遗留下来的服务。很少有 M2M 应用需要此服务。存在一个问题，即使用的 M2M 主机与模拟语音没有很好的接口。

9.4.3　管理服务

M2M 模块供应商提供很多管理服务，这通常是通过预先集成的软件的客户支持。以下部分提供了一些模块支持的示例客户端和服务。

9.4.3.1　设备管理客户端

模块供应商提供的最常见的客户端是一个防伪安全设备管理客户端。设备管理用于移动运营商、服务提供商和最终客户/公司。设备管理功能通常包括在线应用、数据和配置设置的空中（OTA）分布。工业上一个比较流行的设备管理客户端是基于开放移动联盟设备管理（OMA-DM）标准，而不是 TR-069，它被定为宽带论坛联盟，也很流行。一些厂商在此标准之上通过扩展强制性节点支持包括监控节点增加了功能，它会自动触发装置发送一个更新（例如，当一个接收信号强度指示器（RSSI）节点小于已定义的值时，它会触发一个更新）。模块供应商可能提供动态创建节点能力并且管理那些与 M2M 应用相关的节点，不仅仅是模块本身的节

点，例如泵的温度。

设备管理需要考虑的因素包括：

- 支持设备和 RAM/Flash 存储器完整性检查。
- 支持自我诊断和故障管理（下文有介绍）。
- 支持 M2M 应用和非应用软件/空中固件更新。
- 引导配置，即初始配置。
- 协议的安全性和设备的安全，如远程锁定和解除机制。
- 性能，如网络使用率。

9.4.3.2 防火墙更新

大多数供应商提供不同级别的防火墙更新支持。这一般作为设备管理服务的一部分，例如，OMA-DM。然而，并不是所有的供应商都提供 M2M 应用层软件更新（应用运行在模块上或模块外部）。M2M 应用层软件可以用各种语言编写，例如，Java，Python，Lua 或者 C 编程语言。

在初始化模块防火墙之前，注意要确保所有基本认证（例如 PCS 终端认证评估委员会（PTCRB）和全球认证论坛（GCF）），以及在软件上所完成的再认证。然而，M2M 应用的更新（比如 Java，Lua 或 Python 应用），在模块上或模块外运行时通常不需要再次认证。

9.4.3.3 自诊断和错误管理

自诊断和错误管理是很多供应商都提供的一些很有用的服务，它通过一个模块的预集成软件客户端和后端门户网站进入和控制服务。这些服务的主要目的是更快地找到设备和应用设计问题，以便在更早的发布中释放，提高质量。它们在查错硬件甚至判断移动网络领域问题也很有用。与 OTA 性能相关的诊断还可以用来简化设备现场试验过程，有时需要载体认证。自诊断和错误管理服务中一些基本的服务包括：

- 监视器保护——避免锁定软件。
- 报告网络使用情况——CS、data 和 SMS。
- 通过 ICMP 响应“ping”。
- 通过 SMS 命令初始化 PDP 上下文激活。
- 报告设备认证信息，例如，模块/设备/订阅。
- 报告当前服务单元和邻单元 ID，接收信号级别和其他无线链接质量数据。
- 报告无线链接质量数据的存储历史记录。
- 报告和执行 HW/SW/配置文件的设备集成检查。
- 报告电池负荷水平。
- 报告关键事件（例如，重新启动、重置或崩溃）。
- 通过远程命令启动和停止存储。

- 报告指定的 IP 地址。
- 报告位置（假设 GPS 支持）。
- 检查附加到模块上的外围设备数据。
- 通过远程命令重新启动模块。

供应商提供不同级别的安全性防止模块诊断服务的非法接入。

大多数的服务使用专门的协议和客户端，但是 3GPP 已标准化的这些服务在它们的“最小化驱动测试”功能版本 10 中已标准化。这个服务更多地集中于自动化测量功能，收集网络链接质量信息，目的是为了衡量和优化网络和模块的性能。

9.4.4　应用服务

超出管理层服务，该模块供应商可能提供其他类似安全性和定位的应用服务。

9.4.4.1　安全性

供应商用库来提供额外的安全性支持。特性有 RF 拥塞检测，加密套接字协议层，安全英特网协议（HTTPS），加密库和安全数据存储。

9.4.4.2　定位

供应商提供经过测试的和预先集成的库来驱动特定的 GPS 硬件，这样使得客户需要的集成度最小化。

9.4.4.3　其他服务

供应商提供的其他服务包括：

- 音频滤波。
- 双音多频产生。
- 网关服务——动态主机配置协议（DHCP），网络地址和端口转换（NAPT），域名服务器（DNS）代理，端口转发，简单网络管理协议（SNMP）。
- 低功率服务库和专有的 CPU。
- SIM 服务——EAP/SIM 或 EAP/AKA 代理进行身份验证。
- 电子邮件支持。
- eCall。

另外，欧洲电信标准化协会 M2M 技术委员会正标准化一些服务层，例如 ETSI TS 102 689 和 TS 102 690，而且在 TIA TR-50 中，模块供应商终会支持这些服务。

9.5　软件接口

上面描述的服务可以应用到使用软件接口的应用。一般来说，接口为应用控制提供制作、破坏和监控移动连接、发送和接收数据。较好的接口提供控制外设和其他有用的服务。这种模块支持的专用服务协议和控制接口需要反映出全部的服务和

可用的接口，正如上文中所说，它是多样化的。这也导致商业可用软件接口的多样化。本节将介绍模块软件接口的类型。

9.5.1 AT 指令

AT 指令接口装载了七位 ASCII 字符串序列化命令。这个接口原是为发送连续连接而设计，但它也可用于 USB。如今 AT 指令接口是最久远的、众所周知的、最常用的 M2M 应用接口。总而言之，它是最适合小型微控制器的，但也可以用于更复杂的设备。3GPP 在 TS 27.707 规范中提供了标准化的 AT 指令合集，这些标准化的 AT 指令常由专用扩展来补充，用来支持独特的服务和接口，例如网络驱动接口规范（NDIS）（与拨号相对）、GPS 和安装。

尽管 AT 指令的使用很普遍，这种接口仍然有缺点。缺点之一是它一次只允许一个突出的 AT 指令，也就是说，它是同步的。尽管理论上支持，但是异步事件仍不能很好地支持。另外，二进制数据不能直接发送，需要转换成十六进制。AT 指令接口在应用数量上也有一些限制，它能同时直接接入模块。然而，许多 AT 指令接口可以通过使用标准化的多路技术协议来使用。

9.5.2 软件开发工具包（SDK）接口

SDK 接口提供很多功能调用、方法、分类和目标。SDK 的使用和基于操作系统的环境对应，常用在手持移动计算处理设备上。典型地，SDK 运行在外部处理器上，除了在模块支持一个内部执行环境的情况下。一个有名的 SDK 的例子是移动宽带 SDK 在 Windows7 第一次标准化。SDK 支持多样化的水平。一个简单的 SDK 只提供基本的连接呼叫服务，而一个复杂的 SDK 支持很多硬件外设、服务和更高层的协议。

模块供应商提供相同硬件的几种 SDK，因为一个 SDK 是一个独立的操作系统（例如，Windows、Linux、Android、WinCE），而且依赖编程语言（如 C、Lua、Java）。SDK 和一种特别的编程语言连接，因为在某种程度上这种应用会被编译并与 SDK 功能呼叫绑定。一些笔记本电脑厂商和移动网络运营商有特定的供应商支持的 SDK。模块供应商可能要支持许多 SDK，这样大多数供应商不必支持所有的操作系统，只需要支持一种编程语言，而且不必为所有模块提供 SDK。

一个 SDK 提供比 AT 指令接口更多的优势，如：

- 支持事件通知。
- 支持标准编程实践的使用。
- 并行接入：单一通用的 API 可以用于多个并行应用。
- SDK 响应快。
- 二进制数据支持：不需要首先进行十六进制编码，可直接发送二进制数据。

SDK 的问题之一是它们是专有的，这就使得即使它们来自同一个供应商，但客户从一个模块移到另一个模块仍然很困难。然而，有了这种明显的需求，有一些标准化组织为模块创造出标准化的开源 API，例如 GSMA 或 OMA。

9.6　蜂窝认证

不同于其他标准认证，所有传输设备都需要蜂窝认证，而且蜂窝产品也需要电信业和移动网络运营商认证。蜂窝认证很复杂，而且是不断变化的，所以本节只介绍这些认证概念和规则，但不是一套完整的规则。对于模块供应商和 M2M 应用开发人员（或集成商）来说，蜂窝认证是非常大的负载。该行业试图在不影响互操作性的质量的同时通过修改过程和测试程序不断减小该负载。集成商的这种负载如此之高，以至于大多数模块供应商都获得电信行业提出的模块认证的概念。但是即使有模块认证，这种代价仍然很高。集成商所需要的测试数量依赖于模块的集成度水平。集成度越低（例如一个焊接模块），所需要的测试数量越多。基于这个原因，完全集成模块由于有着较小的体积或快速 TTM 的需求这样的优势非常吸引集成商。

9.6.1　电信产业认证

对于基于 GSM 的模块，电信产业认证由两个关联控制，即 GCF（全球认证论坛）和 PTCRB（PCS 终端认证评估委员会）。对于基于 CDMA 的模块，已经建立一种新的论坛，叫做 CCF（CDMA 认证论坛）。电信产业认证一般需要：

- 针对一些技术规范的测试，例如 TS 51.010，使用一个公认的实验室。
- 实地测试，例如驱动测试。
- 质量体系认证机构，例如 ISO9001。

如上文所说，大多数模块供应商获得“模块认证”，以最大程度减少集成商执行的测试。既然集成模块有“模块认证”，集成商仍需要执行以下类型测试（取决于模块形式因素和集成商的实施）：

- 辐射寄生排放。
- 辐射射频功率和接收器性能，例如全向灵敏度（TIS）和总辐射功率。
- UICC/SIM 电子测试案例。

模块供应商必须提供一种机制来将模块置于某种操作模式执行上面的测试。另外，模块供应商还需要提供一种公认的实验室来进行和加快上面的测试。应当指出的是，在使用“模块认证”的时候有一些复杂的时间限制。如果模块与陈旧的测试规范不匹配，也就是说，最新的测试规范有很多新的或升级的测试案例，那么“模块认证”可能需要用最新的合适的测试规范来再测试。

9.6.2 移动网络运营商（MNO）认证

不同于电信产业认证，MNO 认证是非标准化的，所以测试数量、测试范围和测试案例也不同。一些移动网络运营商只执行一些小的子测试，而其他做更多的测试，比电信产业认证有更严格的性能标准。MNO 认证集中于 MNO 网络开发的设备，而实地测试和互操作性测试由 MNO 的网络来实施，不是在测试设备上，例如安捷伦测试设备。MNO 认证只处理完整的产品（不是模块），但类似于电信产业认证，一个模块可以被预先认证，来减少集成商的测试负担。因为存在很多移动网络运营商，所以对于一个模块供应商来说，接收来自所有移动网络运营商的模块预先认证是不实际的。

第 10 章　M2M 通信中的智能卡

François Ennesser
Gemalto S. A. , Meudon，法国

10.1　引言

本章探讨如何以最好的方式来应对 M2M 方面日益敏感的安全和隐私问题，同时最大限度地减少终端设备和管理基础设施的成本。

许多现代通信网络的安全性依赖于一个独立的硬件元素（例如，3GPP 网络中，基于 ETSI UICC 平台的智能卡），以确保提供给终端设备的接入凭据的安全。当服务提供商不能够完全信任终端设备时，该选项还为个人终端设备提供灵活性并解决所有权和责任问题。我们将探讨该模式如何处理 M2M 方面日益严峻的新挑战，同时解决其固有的安全性需求。

10.2　M2M 通信的安全性及隐私问题

本书的第 8 章考虑了 M2M 相关的一般安全性问题。当 M2M 通信背景下的安全性继承了以人为本通信系统的大多数原则时，一些新的约束条件增加了额外的安全性要求，从而增加了系统的复杂性。

在网络层面，需要以负担得起的方式对大量的连接设备进行有效管理，并可使用广播和多播技术加强对设备管理基础设施与组寻址能力需求的建立。

此外，M2M 设备的多样性可以通过一个共同的 WAN 创建委托大多数数据处理和协议转换功能的需求连接至媒介网关。

在设备层面，M2M 通信设备本身可以是复杂系统的一部分（如机动车辆），其不容易接入。在其他情况下，业主机构无人值守该设备和/或该设备位于难以到达的地方，其造成的结果是派送维修人员将过于昂贵。因此，当考虑预见的 M2M 应用的广泛多样性时，需要重新考虑应用于常规移动终端的一些假设：

- 现有设备相关的服务订阅应防止被一些意想不到的目的重新使用。在设备无人值守的位置需要适当的安全对策，如智能电表、交通灯或自动售货机。
- 一些规章如欧盟普遍服务指令（EUSD）[EUSD]，进一步要求不论用户决

定什么时候更改提供商，都应在字段中交换订阅数据。在 M2M 设备的生命周期中，这种情况的发生可能不止一次。

在工业应用中涉及大量的无人值守设备，服务提供商之间的订阅需求可能会发生变化，必须需要远程管理解决方案来满足这一需求，因为相关的物理干预在潜在的广泛范围和地理分散基础上的成本被禁止。另一方面，个人消费设备上的应用或用户隐私处于危险之中的各种业务中的预付模式，与远程管理解决方案相比，用基于 SIM 无线移动网络的传统“弹性漫游”情况可保持高度契合，因为它具有便利性和成本优势。在这种情况下，该订阅被嵌入在智能卡中，可以根据需要很容易地从一个设备到另一个设备进行转换。

这突出强调了一个事实，即对于处理 M2M 应用的巨大差异性没有一个“通用”解决方案。评估最适合的解决方案需要考虑市场的具体情况。而安全的远程管理功能提供的灵活性应成为 M2M 网络中的战略性方案。

此外，在 M2M 环境中往往需要特定设备的特性，例如：

- 设备寿命：在某些领域如智能计量，期望设备寿命可长达 20 年。这对于非主要供电设备如某些气表、水表或一些移动设备特别成问题。在这样的时间帧内，需提供极大的灵活性以适应计算机和通信技术的发展，并解决新的安全威胁，如加密算法可能发生的演变和接入网络技术在产品生命周期间的变化。
- 环境条件：这包括存储和操作温度或湿度，以及暴露于化学腐蚀之下多种情况，如碱性空气或如冲击和振动的机械约束条件。这些因素结合在一起，使期望的设备寿命的评估更具挑战性。

同时，一些 M2M 应用，如智能电网或医疗设备，在安全性（和可靠性）方面比普通通信服务有更迫切的需求，因为它们会影响更重要的人类需求。

最后，从用户周围的设备（如家庭能源、水表、汽车和医疗设备）中收集数据量的增加有可能危害个人隐私权。因此，除了满足传统安全需求，还需要设备或网关（潜在的计算强度）的机制来保护匿名的用户和用户的隐私。如果不解决这个需求，可能会危及一些应用的实现，如荷兰已出现这个问题，由于消费者担心隐私问题，国会开始拒绝法律强制采用智能仪表或自动道路定价技术。而在一些应用中，一个众所周知的方式是使用匿名预付订阅保护顾客的匿名，这种方式应得到保留。

10.3 采用基于硬件的安全解决方案的理由

任何基于软件的安全实施，无论是在嵌入式设备、移动电话、个人电脑或数字助理，都对潜在的软件攻击开放，如木马、蠕虫或病毒。此外，逆向工程技术，如提取程序代码和拆装/调试方法，在与其他应用共享的软件环境中大大地简化，从而导致潜在的敏感秘密组件如算法、私钥和其他被假设是安全信息的暴露。因此，

基于硬件的机制总是需要提供足够的保护。这包括简单的物理攻击无法读取或改变的防篡改存储器，对重要操作进行保密的物理保护机制，以及免于传统攻击的硬件探测器。但是对于秘密的保护只使用专用硬件是不够的。确保执行环境以防潜在的侧信道攻击，如简单或差分功率分析，分析电磁辐射来推断处理器操作的数据，其执行需要特殊的技能，并在实施安全算法时需巧妙地编写软件，以迷惑侵入式或非侵入式的攻击。由于标准化不能处理该实现问题，它们必须由一个专门的行业认证以成熟的方法进行处理，如通用准则评估保证等级（ISO 15408）或北美 FIPS。

我们可进一步将基于硬件的安全解决方案分为三类：可移动的独立安全要素，固定的独立安全要素和嵌入式（非独立）硬件。安全要素给设备提供了安全功能，如存储密钥和执行加密功能。安全要素可以是可移动的或可焊接到设备上。移动设备中的 SIM 卡是可移动的独立安全要素的一个很好例子。用户可以从设备中取出 SIM 卡，并插入一个新卡。将安全微控制器（如智能卡芯片）嵌入一个安全设备，如 USB 身份锁，这是固定的独立安全要素的一个很好例子。由于一些安全解决方案内置于设计之中，某些硬件可能无法显示独立安全要素。这些基于软件和基于硬件的不同解决方案具有不同的特性和功能。表 10-1 为这些不同解决方案的一个对比。接下来的几节对该表的内容进一步解释和说明。

表 10-1　比较评估不同的安全解决方案

		可移动的独立安全元素	固定的独立安全元素	内置（非独立）硬件	基于软件的安全
解决方案的一般安全性					
	物理	中	高	高	低
	逻辑	高	高	中	低
算法					
	算法安全性	高	高	中①	低①
	资源所有者自定义算法的可能性	高	中	低①	低①
	更新算法的设备	高	中	低①	低①
证书					
	检索证书的难度	高	高	中①	低①
	服务提供商数据的保密（设备制造商不知道数据）	高	高	低①	低①
制造、部署成本		高	中	中	低

（续）

		可移动的独立安全元素	固定的独立安全元素	内置（非独立）硬件	基于软件的安全
个性化					
	个性化的容易度	高	高	低①	低①
	在个性化过程中的安全性信任度	高	高	低	低
订阅管理的可移植性		高	中	中	中
防盗					
	防盗方案的信任度	中	高	高	低
人工干预					
	没有人工干预的使用容易度	低	高	高	高

① 状态取决于终端受保护的方式（例如，标准的或专有的解决方案）。

10.4　独立安全要素及可信环境

10.4.1　M2M 设备可信的环境

10.4.1.1　需要安全“环境”

在一个开放平台上，对敏感数据进行安全的存储、处理、输入和输出是至关重要的。这就是为什么出现确保通用计算平台安全的举措的原因，如可信计算组（TCG）。

正如上面所解释的，需要一个防篡改的环境，以保证给执行敏感操作和存储凭据提供足够的保护。设备需要足够的安全，否则它的通信模块将出现多个弊端。例如：

● 已制定的安全标准一般很少有适用于通信模块或 M2M 设备的。目前，最著名的解决方案，如 TCG 相关的工作，没有真正解决对底层硬件的攻击。从制定方法上讲，“安全环境”或“受信环境”的概念与公认的安全级别无关。此外，如上文所述，正确执行安全功能需要专业技能，不是传统意义上没有具体安全专业知识的公司所能使用的。

● 不同实现的功能也不尽相同。即使就确保部分模块或设备的安全达成协议，实际的安全级别也会依赖于功能的设计和实现。如果应用到整个设备/模块的计算

环境，那么所需的硬件实现将是昂贵的。而且，不能保证所有特殊的实现总是会正确使用现有的保护机制。

漫游时，会涉及不同的服务提供商，在现代通信网络中，安全链中最薄弱的连接（针对最脆弱的设备的攻击）由一个服务提供商造成，其可能会影响到所有相关的服务提供商。因此，需要依靠广泛公认的安全认证计划，如通用标准，这对于模块/设备综合的安全解决方案更为重要。如本章后面详细介绍的，一个独立安全模块具有非常明显的优势。

然而，将内置于通用处理器与专门的独立硬件的受信环境相比较，如智能卡，除了为敏感数据提供安全存储，如加密密钥，都可以被设计为先进加密算法支持的相似的功能、随机数生成器、密钥生成及加密/解密和签名方法。这些都可用于为各种网络和应用提供磁盘加密和身份识别功能。它们之间的主要区别是，受信环境中通常包括的信任的根，执行加载到通用处理器的软件模块，使其计算签名。然后将这些签名与安全存储的参考值进行对比，以提供完整性验证。只要存在一个内置的信任根提供受信的签名，那么受信签名就不需要内置于受信环境本身的安全环境内，并可在一个独立安全要素内容易地执行。

另一方面，独立安全要素，如智能卡，如今提供一种安全的专用微处理器（嵌入式或可移动），即使在字段中设备部署之后，它也可以安全地将新的应用程序化并更新，这都要归功于虚拟机的支持，如 JavaCard 平台。此功能为智能卡在各种场景中的成功应用打下了坚实的基础，如支付卡、公共交通通行卡或通信网络安全模块。这种解决方案的好处是当服务提供商不拥有主机设备本身时，大力加强对其接入凭据的保护。实际上在这种业务情况下，服务提供商之间需要如下的良性竞争要求：

- 服务提供商的远程管理数据必须与设备的配置和应用管理无关。
- 保护服务提供商资产的加密算法必须与设备制造商无关。

加载于智能虚拟机的应用，以及相应存储数据，使用标准和安全机制实现独立于主机设备的远程管理功能，这些我们将在后面作详细讲述。

10.4.2　可信未知设备：需要安全认证

10.4.2.1　M2M 设备认证

在 M2M 背景下，设备或其安全模块认证程序面临以下困难：

- 定义边界部分的安全。
- 定义每个特殊行业的特定保护配置文件。
- 安全目标范围的风险可能比较大：
  - 安全目标越大，认证要求越困难，以及由此产生的成本越高。
  - 认证的复杂性直接受环境冲击的影响（例如，更多的参与者、更详细的过

程、更多的风险），这些进一步增加了成本。

–将维护考虑在内的需求具有更深远的影响。

为了确保安全要素的完整性，至关重要的是确保供应商方面制造环境的安全性。事实上，除了设备本身的认证，在最初的设备制造期间，必须要执行可信凭据的一些配置，以使服务提供商可以信任的设备作为能够保护自己接入凭据的安全容器。

为了防止这些凭据暴露，需要验证所有的人、设施和相关操作凭据的进程，以在字段中提供值得信赖的设备进行准备工作。

由于这些进程要遵循特定的行业法规，如支付卡行业数据安全标准或 GSMA 移动通信的安全认证方案，所以要将该类进程进行管理，在内部程序中整合，并在如智能卡制造商的安全专家的生产设施中实现。另一方面，对于一个还没有熟悉这些问题却试图遵循该进程的机构，该过程是非常昂贵的。

值得一提的是，GSMA 已经确认需要启用远程个性化的 M2M 安全要素，这需要更改或适应它们的验证方案。

10.4.3 智能卡模型的优点

在 M2M 设备实现和生产中建立一个不忽略认证和验证过程的可信的安全链。该过程增加的成本与基于智能卡的解决方案相比没有竞争力。这些依赖于定义明确的、大量生产的独立安全要素，都可以很容易地在设备的设计中集成，并以每年超过 10 亿的庞大数量传递到其他行业。智能卡在一个不断增长的业务领域范围，从银行到移动通信的数字识别，其已经证明了自身的适应能力。

在 TS 102 221［TS102221］中，ETSI TC SCP 已指定应用无关的 UICC 平台提供可用于将独立安全要素嵌入 M2M 设备的通用的多应用智能卡平台（见图 10-1）。

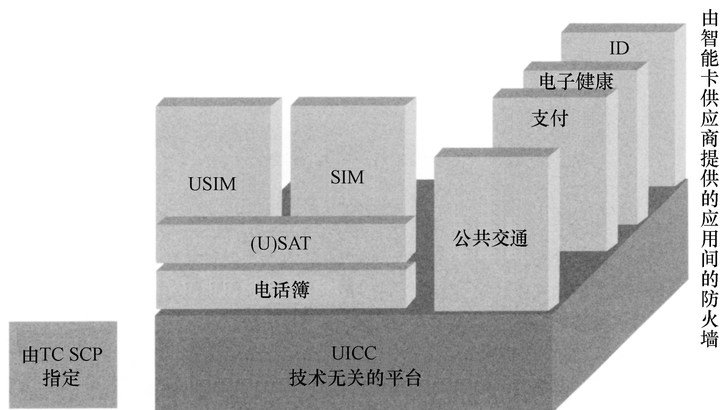


图 10-1 ETSI UICC 平台

此平台提供了一个可远程管理的高度安全环境，并将向本地连接设备提供安全服务；UICC 本身作为一个安全应用平台执行管理功能。更具体地说，UICC 综合了以下特征：

● M2M 应用的一个特定扩展（ETSI TS 102 671）［TS102671］，为嵌入式应用定义特定的形式因素并提供特定的环境和使用寿命特性。

● 虚拟机 API（在 ETSI TS 102 241 中指定为 JavaCard）［TS102671］和扩展卡应用工具包（CAT）（ETSI TS 102 223）［TS102223］，使卡上的应用与主设备或其通信模块所提供的功能相互作用，同时提供防火墙保护不同小型应用之间的机密。这样的虚拟机已经达到了一个通用标准评估保障等级认证的 EAL4＋。

● 根据 ETSI TS 102 225［TS102225］和 ETSI TS 102 226［TS102226］，将安全远程管理解决方案的文件和应用装在卡上。远程管理通道在 UICC 自身建立一个安全终点，从而在主通信设备等级防止敏感信息不受损害，并支持多种载体和协议，以达到灵活应用的目的。此外，依赖于从 Global Platform 规范到特定的安全域，为每个应用提供独立的管理功能，从而保护它们的敏感数据的机密。

该平台还提供了以下可选的扩展接口（见图 10-2）：

● 一种现代的、具有更高数据速率及更通用的芯片内部的 USB 接口（ETSI TS 102 600）［TS102600］，使用 RST、CLK 和 I/O 接点，可替代传统的串行智能卡接口。

● 在主设备的非接触模块的单线接口（SWP：ETSI TS 102 613［TS102613］）与主控制器接口（HCI：ETSI TS 102 622）［TS102622］；

● 一个 IP 扩展允许在 TCP/IP 网络中轻松地集成，为本地和远程连接提供客户端和服务器运作模式（具体地在 ETSI TS 102 483［TS102483］）。

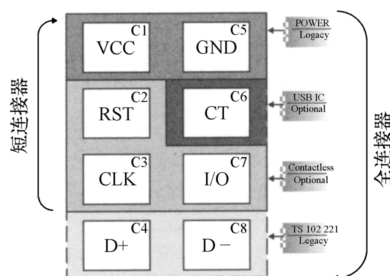


图 10-2　UICC 接口接点分配

该平台已经作为一些通信网络技术安全证书的位置标识符，由基于 UICC 网络接入应用规范的下列机构进行标准化：

● 3GPP 使用 3GPP UICC（3GPP TS 31.101）使 USIM 应用（3GPP TS 31.102）适用于网络接入，且 ISIM 应用确保 IMS（3GPP TS 31.103）上的服务安全。

● 3GPP2（CSIM 应用：3GPP2C.S0065）。

● ETSI TETRA（TSIM 应用：EN 300 812）。

● WiMAX 论坛（WiMAX SIM 规范：http://www.wimaxforum.org/sites/wimaxforum.org/files/technical_document/2009/09/WMF-T33-114-R015v01_WiMAX-SIM.pdf）。

世界各地的许多国家已证明，基于智能卡的单独配置提供的灵活性对于上述技术的成功配置起到了促进作用。

当然，独立安全要素，如 UICC 和其主设备之间的接口必须要进行标准化。否则，在某些情况下，会被攻击者窥探。但这样的安全要素依赖硬件协作处理器将大量可编程安全存储器与先进的加密功能相结合，从而在较低工作频率下使电力消耗最小化的情况下提供快速的计算。使用即时 API 功能，结合高度灵活的应用，开发和管理虚拟机环境，这使得机体内部包含了所有敏感的安全功能，避免了任何未受保护的安全信息与主设备的交换。当这一切措施还不够充分时，ETSI TS 102 484［TS102484］可以建立一个安全通道与主设备进行通信。

10.5　M2M 环境下特定智能卡属性

10.5.1　可移动智能卡与嵌入式安全要素

一个可移动智能卡使用 ETSI TS 102 221 指定的形式因素之一（见图 10-3）或 ETSI TS 102 671 指定的带有连接器的小型化 MFF1 形式因素（见图 10-4），可以提供一个真正便携的订阅解决方案，因为 ETSI 指定的标准化智能卡接口为 UICC 平台提供与所有接收设备的通用互操作。它还提供了所有现有的工具确保 UICC 的空中（OTA）管理的安全性，每当订阅相关参数时都需要进行更改。

消费设备应用经常需要用户能够在不同时间的不同设备中使用相同的服务订阅，或不同服务提供商使用单一设备。最好在 TS 102 221 指定的传统形式因素之一中使用物理的可移动 UICC，在这样的应用中，此方法是最合适的。另一个使用可移动 UICC 的优势是：尤其在具有很长生命周期的设备中，能以合理的成本解决随着时间的推移可能出现的新的威胁，使安全模块升级（加密保护、处理器和算法）。十年内，安全是一场持久战，新的威胁和工具被发现，以前的安全实现需要升级。

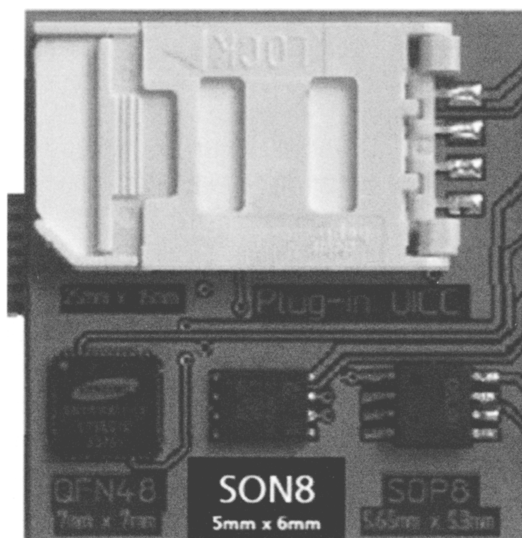


图 10-3　与 MFF2（又名 SON8）形式因素相邻的连接器里的可插入智能卡

虽然可移动 UICC 能被窃取，但有几种解决方案可以应对这一威

胁，并使其对于窃取者没有用处。当服务需求需要保存 UICC 可接入性时，可使用这种解决方案。UICC 的可接入性，是固定的或是可移动的，完全取决于整个设备设计：被放置的地方和其机器的类型（汽车、仪表、自动售货机等）。实际上，一些工业 M2M 设备设计使 UICC 几乎不可能被用户接入，以阻止 UICC 的窃取者。这是因为可移动 UICC 的“弹性漫游”优势是不再需要这类应用。在这样的情况下，使用一个机械连接的 UICC，例如在固定 MFF1 或 MFF2 模块中的启用，就是指定在 ETSI TS 102 671 中使用远程订阅管理解决方案来提供恰当的切换。

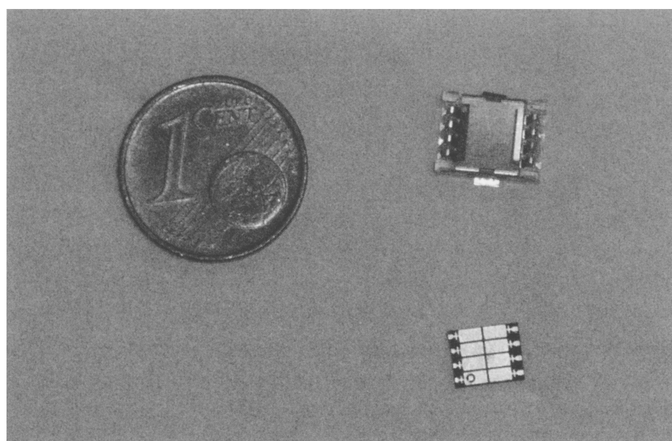


图 10-4　TS 102 671 的多功能 MFF1 形式因素与其连接器相邻
（图中所示的 MFF 组件由 Gemalto 提供，连接器由 Yamaichi 提供）

非移动 UICC 需要遵循规范的远程管理解决方案控制服务提供商之间的自由竞争。虽然在今天，UICC OTA 标准化不支持远程创建一个新订阅或远程更换卡上现有订阅的可能性，但其仍然提供了一种在设备中有效管理现有订阅的方法。一些特有的模式使订阅在字段中发生变化，如白色标签 SIM 最初配置有多个订阅并由中央集权管理，这已在 Brazilian Departmento Nacional de Transito（DENATRAN）为汽车通信模块提出的模型中出现。ETSI SCP 正在启动一项具有更加灵活特性和可互操作性的模型的标准化工作，如本章后面所述。

不与远程管理方案结合时，某些情况下，可在固定 UICC 上更换整个模块提供一个可接受的选择方案，保持整个模块的低成本。

10.5.1.1　M2M 安全要素分布及物流影响

对于非移动 UICC，物流和部署与传统可移动智能卡有很大的不同。这样的安全要素一般不交付于服务提供商，但交付于将其纳入 M2M 设备的 M2M 设备制造商。由于物流方面的原因，在设备制造产业链的末端一般都需要使卡呈现个性化，所以，在此阶段，该卡可能尚未被配置服务凭据。

更复杂的分布模型是智能卡被发送给初始发行人，然后发送给零售渠道，并最终发送给终端客户，智能卡最终被插入设备，此分布模型导致成本的明显增加，并使 M2M 因此而避免使用此模型。与其硬件成本相对比，可以估计向 M2M 客户供应卡的网络成本（身份和凭据配置）是非常显著的。

为进一步降低成本，我们可以设想一下下列要素：

- 在配置过程中减少智能卡成本，通过：

–提高效率。

–增强扩展性。

–减少配送成本。

- 重复使用智能卡并向毛细网络中的多台设备提供安全性。
- 减少网络方面的成本，通过：

–在网络中使用典型的 IT 数据库技术，例如，轻量级目录接入协议（LDAP），通用十进制分类法（UDC）。

–改善许可模型，使存储容量不作为主要的成本要素，而使处理能力成为制约因素。

–减少处理负荷较少的整体连接/断开事件，并尽量减少进入数据库的独立设备的总数，例如，使用设备分组或本地委托。

无论用哪种安全方案解决设备的个性化和服务引导问题，M2M 设备的安全和配置方式成为一个重大的挑战，尤其是在部署的设备数量急剧增加的情况下，基于独立安全要素的解决方案能够充分利用智能卡行业发展的大量已有的物流专业知识处理移动通信网络中的约束条件。

10.5.1.2 可移动 UICC 逻辑设备配对

一个可移动的 UICC 可被绑定到机器或机器组，其被插入一个配对机制，如 ETSI TS 102 671 中所指定的，没有必要对 UICC 插入的位置进行物理保护。这样的 UICC 将无法在任何不属于既定组的设备中工作（或不能成为它的初始目标主机）。

一种简单的“恢复”锁定机制，可与将有特定身份（IMEI，IMEISV，MEID 或 ESN）的 GSM 终端与既定的 SIM 卡绑定的 SIM 锁定机制相媲美，但可使用其他工作方式：在 GSM 词汇表中，用“IMEI 锁”替代“IMSI 锁”。这需要 UICC 采用主动功能（也就是，支持 CAT ETSI TS 102 223），否则，由于将智能卡设计为仅执行其主机命令的形式，例如，读取 IMSI，而不是请求行动。即便如此，如果不能正确执行该机制，那么它在一些方面可能会被忽略，例如，通过使用伪造终端或中间人机制允许向被盗智能卡呈现所需的身份。

10.5.1.3 UICC 和其主机间的安全通道

一个更安全的替代方案是在卡和终端之间即时建立安全通道的基础上，使用 ETSI TS 102 671 指定的锁定机制。假设主设备本身提供某种受信任的环境，根据

安全通道规范 ETSI TS 102 484 ［TS102484］，允许安全存储并利用与该卡加密通信的安全密钥。

根据安全需要的应用，TS 102 671 允许 UICC 与终端之间最初产生的没有真正确保通信的安全关联。否则，必须使用 ETSI TS 102484 中迫使卡与终端之间的所有通信都必须加密的平台到平台的选项。

注意，ETSI TS 102 484 还提供了一个选项，其使用应用到应用的安全通道，对基于敏感 UICC 应用相关的通信量进行选择性加密，且此选项与其他设置无关。此外，TS 102 484 安全通道不仅解决了传统通信的串行接口问题，而且可通过 TS 102 600 的 USB 接口进行通信，包括互联网协议格式的通信。

10.5.1.4　UICC 服务限制

对于满足上述要求的设备和 UICC，仍可使用一种组合的业务流程和安全措施防止对网络和系统进行未授权的接入，通过快速检测可疑活动，最大限度地减少嵌入式设备中服务盗窃的风险，通过：

● 把服务控制在既定嵌入式应用的最低水平，例如，GSM（U）SIM 的呼叫限制功能可用来将呼叫服务限制在既定的唯一一方。

● 对可预见的嵌入式应用开发一种正常使用模式，通过：

– 将通信量限制于合理应用的需求之下。

– 从正常模式触发警报的高使用率和偏差。

● 使用嵌入式应用提供安全的、可行（例如，通过使用 IPSec）的、私人专用的 APN 单独用来进行嵌入式服务。

注意，即使使用纯粹基于软件的安全性，在 M2M 设备上执行通信应用的订阅凭据仍然存在被盗的风险。此种盗窃虽不像物理盗窃一样具有可见性，但这些数据的曝露将比对具有安全订阅的智能卡的盗窃更具破坏性。

10.5.2　UICC 抗环境制约

可以在各种环境中使用 M2M 设备，如某些 M2M 设备可用于具有极端温度、湿度、化学成分或机械暴露的环境。此外，在某些应用中，使作为整体的设备寿命最长，这是非常重要的。

环境的配置文件通常会以如任何相关（可移动的或固定的）智能卡的相同方式影响整个 M2M 设备。M2M 设备的所有组件也会受到影响。但在某些情况下，可移动 UICC 可能具有与设备的其余部分稍不相同的条件，例如，额外的壳体可使部分设备在湿度中得到很好的保护，或可将 UICC 阅读器放置在更舒适的环境之中，如放在汽车的仪表板而不是引擎的隔间。

ETSI TS 102 671 对于环境条件提出了一种分类系统，其满足基于下列参数的 M2M UICC：

- 操作和存储温度。
- 水分和回流条件。
- 湿度。
- 化学腐蚀和可能的摩擦腐蚀。
- 振荡。
- 冲击。
- 存储器中的数据保存时间。
- 最低更新要求。

这种环境分类系统使各行业部门在自己的特定环境中，指定适合于智能卡使用的目标配置文件。

一般使用加速方法在渐短的时间段内集中约束条件测试所支持的需求，对于产品来说，预计将在整个预期寿命内承受这些约束条件。ETSI TS 102 671 中规定了适用于各类测试的测试规范。

10.5.2.1 寿命

由于各种使用情况和市场模型各不相同，故 M2M 设备期望的寿命从两年（汽车租赁车队管理）至 20 年（智能电表）不等。在许多工业应用中，往往期望设备的寿命在 10 ~ 15 年之间。

对于 UICC，其寿命不仅取决于数据保留时间和其非易失性存储（EEPROM 或 Flash 技术）所支持的读/写周期数量，而且取决于所受的环境约束条件的影响，如存储和操作温度、湿度等。

对于可移动 UICC，当使用适当的材料时，触点的氧化不是一个决定性的因素。更重要的一般是可移动和插入周期的数量，但在要求严格的应用中（如消费者参与的设备），通常每隔几年就进行更换。

至于读/写周期，在寿命方面的转换很大程度上取决于每个人的使用情况和内部产品的实施。如今，UICC 芯片支持硬件读/写周期 100000 ~ 500000，但低级的损耗均衡机制可进一步用于防止任何特定的存储单元过早失效。考虑这样一个例子（给定区间范围）：在一个给定单元，每小时都进行一个循环，硬件寿命将（依书写角度来看）从 11 ~ 57 年不等。这意味着硬件技术不是制约因素，而适当的损耗均衡机制对产品寿命的影响最大。当不执行适当对策时，在频繁更新的位置很容易发生早期局部存储器故障。高效损耗均衡技术必须对用户透明，因此在卡操作系统的较低层执行。

ETSI TS 102 671 建议通过验证评估用于频繁更新的 UICC 信息支持选择 100000、500000 或甚至 1000000 更新周期的功能。这可以与选择存储器保存期 10 年、12 年、15 年的要求相结合。

10.5.2.2　存储和工作温度暴露

ETSI TS 102 221 和 TS 102 671 提供测试方法以评估 UICC 在下面温度范围内是否适合操作和存储：

- −25 +85℃。
- −40 +85℃。
- −40 +105℃。
- −40 +125℃。（最后一组条件涉及最恶劣环境下的具体设计限制）。

10.5.2.3　暴露于湿度之中的生产和寿命

TS 102 671 提供以下功能：

- 在制造过程中，湿度/回流条件分类适用于固定的 UICC（对于可移动 UICC，反而应该考虑连接器的微腐蚀要求）。
- 在潮湿环境下的工作状况。
- 在碱性气体中的腐蚀。

10.5.2.4　冲击、振动和其他机械限制

ETSI TS 102 671 使 UICC 配置满足 JEDEC（美国电子器件工程联合委员会）对于汽车应用定义的振动规范［JESD22Vib］和冲击条件规范［JESD22Shk］。

在 ETSI TS 102 671 中设计 M2M UICC 形式因素的目的是为了满足交通运输设备所需的严格的振动和冲击限制，如汽车。除了用于连接的电接触点，它们还提供了旨在牢固地锚定到其主机电路板的大量独立的机械垫。

然而，主要要注意机械限制，如冲击或振动，不妨碍可移动 UICC 的使用，原因是，即使在最恶劣的机械环境中，仍可利用鲁棒的 UICC 阅读器确保可靠连接。由于双方的 MFF1 形式因素和其连接器的设计目的是为解决这类制约因素，所以阅读器对于 TS 102 671 的 MFF1 格式是最困难的。但即使是一些小型 UICC 阅读器，仍可利用其合理满足要求苛刻的机械限制。

10.5.3　用于无人值守设备的自适应卡应用工具包

可以在虚拟机上应用 UICC，如 JavaCard，并向其主动使用功能（CAT，ETSI TS 102 223［TS102223］）提供 API（ETSI TS 102 241［TS102241］）。这是 UICC 在移动通信网络应用成功的关键因素，在这里，通信运营商利用这个平台功能，为客户提供增值服务或优化特定功能，如漫游功能。在 M2M 市场中，预期这些 UICC 平台功能将继续由（通信或 M2M）服务提供商作为一种竞争优势。而在 M2M 环境中，当部署基于 UICC 的应用时，必须将一些差异性予以考虑。

主要要考虑的是，移动电话业务中依赖于移动手机的用户界面（尤其是屏幕，键盘）启用的客户互动的许多增值服务。另一方面，大部分 M2M 设备是无人值守的，尤其是在工业应用中，并且有些 M2M 设备没有（或大大降低了）界面功能。

这就是为什么最新版本的 CAT 规范（ETSI SCP 和 3GPP Release 9）包括终端特定配置缺乏某些功能的原因。

- 没有显示或其他用户信息功能。
- 没有键盘或其他用户输入功能。
- 没有音频预警功能。
- 没有语音通话功能。
- 不支持多国语言。

其结果是主动型工具包命令在其他方面不适合或仅有一部分支持依赖于这类功能（也就是说，有一些限制）在这样的终端中。但可以依赖通信功能开发有用的应用。

10.5.4　使用工具包命令到达 UICC 外围设备

要考虑到的另外一个因素是 M2M 设计可能会与手机设计在一些方面有所不同。虽然现代手机往往显示出一种双处理器架构（数字基带调制解调功能与应用处理器相分离），UICC 一般通过其串行接口（ETSI TS 102 221［TS102221］中定义）仅与调制解调器保持连接，适当地处理卡的积极需求。在一个 M2M 设备中，可以很容易地将设备中的 UICC 直接接口应用处理器，例如，通过使用芯片间的 USB 接口（在 ETSI TS 102 600［TS102600］中指定）。但由于上述传统，预期许多 M2M 设备将保留这样的架构：UICC 仅与通信模块通过串行接口相连接，该模块本身通过一个接口连接到设备的应用处理器，其接口一般基于 AT 命令规范（例如，在 3GPP TS 27.007［TS27.007］中），如图 10-5 所示。

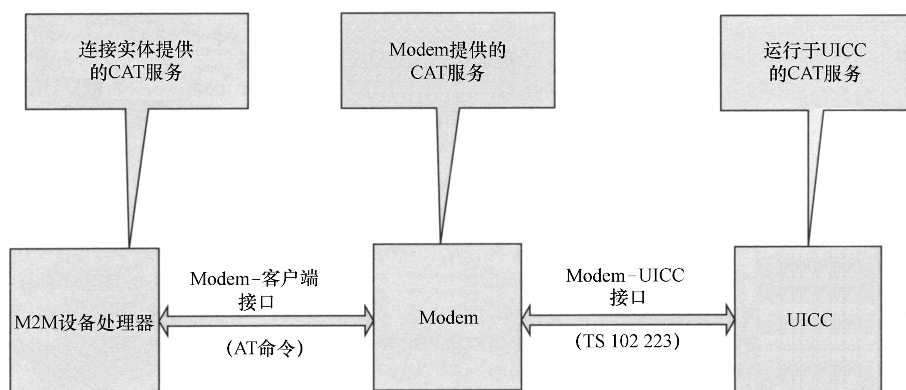


图 10-5　在 M2M 设备中使用工具包服务的 UICC 应用

在 M2M 设备中，若主动型 UICC 应用能够与设备本身的应用处理器进行交互，这将大有益处。因此，在 M2M UICC（其可能已持有无线 WAN 传输网络接入权

限）只具有通过通信模块的 AT 接口与应用处理器间接连接的架构中，通过 AT 接口需要传送工具包命令。这一需求已得到解决，由 ETSI SCP 通过改变 TS 102 223 版本 9 的方法，使其通过对 AT 命令集仅有极小改变的 AT 接口传输 CAT 通信量。例如，所连接的实体，M2M 设备的应用处理器，如果必要的话，可以被识别甚至被认证，并指示所支持的一组 CAT 功能，其提供一种调制解调器本身可能已带有的补充功能。

10.5.5　第三方应用的安全及远程管理

M2M 和移动通信方之间的另一个区别是，参与 M2M 业务协议的一些实体，如 M2M 服务提供商和接入网络运营商，通常需要在相同的 M2M 设备中保存自身的凭据和订阅。UICC 平台已设计成为支持多种应用的平台，以使 M2M 设备中一个单一的安全要素就可以确保整个相关订阅的安全。然而，也许只有一个实体，即设备雇主拥有该 UICC。不同的保修和责任影响，取决于安全要素保修是否绑定到 UICC 拥有的实体或绑定到设备上，如集成于汽车中。此外，第三方可能允许远程改变其 UICC 功能，而无需 UICC 所拥有的实体许可，这取决于第三方提供的服务所扮演的角色。例如，网络运营商的网络接入应用被保存于一个可能仅允许修改连接参数的 M2M 设备提供商所拥有的 UICC 之中。

为了解决这些问题，GlobalPlatform 卡规范版本 2.2［GP22］和其修正案 A［GP22A］提供具有很大灵活性且适应于各种不同模型的功能。在 UICC 平台中，ETSI TS 102 225［TS102225］和 ETSI TS 102 226［TS102226］所支持的这些规范，提供在智能卡上独立管理多个领域的功能，每一种规范都代表一个潜在的不同卡外实体且由其自身的一组凭据进行保护。这使得每个应用提供商借助于一个安全（OTA）通道提供完整性、机密性和身份认证，从而单独管理其安全域。这些安全域对于加载、安装和个性化应用进行远程管理，而不会影响到其他用于远程管理的安全域和接入网络的保密性。在卡上建立安全域层次结构来表示潜在的复杂的业务关系，同时保留发卡机构的控制权。发卡机构可以选择自己或将安全域管理委托于第三方，从而对该卡的内容进行管理，使应用提供商在卡上通过（第三方）网络可以充分操作和管理应用，同时保存所有相关卡机密内容（如果需要的话，例如，对于支付相关的应用）。加载应用权限可由一个卡上代表自己的安全域的独立监管部门进行处理。这包括下列所有可能的情况：

- 发行中心：仅允许发卡机构管理卡内容。
- 委托管理：发行者保留加载第三方应用的控制，但相关的第三方可以检查该加载并在其安全域执行卡内容管理。
- 双重管理：多个实体在各自的安全域被授权执行卡内容管理。

另外，无论是在基于内建密钥生成的拉动模式，或是在基于使用临时密钥的推

动模式中，都启用了一些解决方案创建和处理新的安全域问题。

在由接入网络运营商管理的单个 UICC 应用和由 M2M 服务提供商管理的其他应用中，这些能力是必不可少的。

10.6 智能卡在 M2M 环境中的未来演变

10.6.1 基于集成电路的 M2M 服务标识模块应用

基于 UICC 应用（在 ETSI TS 102 221 意义上的第一级 UICC 应用）管理接入 M2M 服务层的规范仍有待于在 ETSI SCP 内进行完善。此“M2M 服务识别模块”（MSIM）应用连同网络接入应用（如 USIM 或 CSIM）可以相同的方式在同一 UICC 中进行操作，如 3GPP TS 31.103 中指定的 ISIM 应用用于确保 IMS 接入。这样一类规范是必需的：可以提供一个存储于 UICC 中的相关数据结构和相关操作程序的可互操作定义。该规范应由特定 API 和工具包命令扩展来完成，使其与工具包小程序协同工作（在 ETSI TS 102 221 意义上的第二级应用），从而满足特定 M2M 垂直市场的需求。

10.6.2 UICC 的互联网协议集成

ETSI TS 102 483［TS102483］可通过下列标准化机制在 TCP/IP 基础设施中使 UICC 平台的集成变得非常容易：

- 分配一个 IP 地址使其集成于主机终端的本地 IP 网络（IPv4 或 IPv6），而无需用户交互。
- 在网络上发布和查找可用的服务。
- 在设备中通过 TCP/IP 解决设备和应用问题。

必须要克服 UICC 继承的传统 SIM 卡协议的局限性，如无法接入本地连接至主机终端的设备或驻留于主机终端中或本地连接设备中的应用。这就是为什么 IP 框架最好协同 ETSI TS 102 600［TS102600］中指定的芯片间 USB UICC 接口工作的原因。虽然 ETSI TS 102 221 的传统 UICC 接口通过使用承载独立协议（BIP）功能提供的代理服务可能仅支持 ETSI TS 102 223 的 IP 连接性，但 ETSI TS 102 600 的芯片间 USB 接口使 UICC 支持完整的 TCP/IP 协议栈。

上面［GP22］中提到的 GlobalPlatform 2.2 规范已定义了一个网络框架，作为对本规范的进一步补充，此网络框架能够确保远程 UICC 配置文件和应用管理在基于 HTTP 的 TCP/IP 网络上的安全性。目前，在最新版本的 ETSI UICC 远程管理规范 TS 102 225 和 TS 102 226 中支持该范式。此外，开放移动联盟已经开发了一种智能卡服务器规范［OMASCWS］，其在 IP 网络中，利用 JavaCard 虚拟机功能，为基

于 UICC 服务的部署提供了一种强大而灵活的框架。

此外，ETSI SCP 以及 GlobalPlatform，从旧的基于 SMS 工具包应用和远程管理框架到 IP 世界，基于互联网方面的 TCP/IP、HTTP/HTTPS 和其他相关协议，其完成了一个完整的迁移。ETSI SCP 工作将通过 IP 网络及利用通常称为“Web 2.0”技术的 IETF 发展，从而支持设备和其 UICC 应用之间的安全通信。GlobalPlatform 工作将通过一种周密可靠的方式解决智能卡集成于通用 IP 网络的问题，根据相关的利益和潜在的风险考虑所有相关的技术。

在 ETSI SCP 中将完成整个工作包基于新 JavaCard 3 引擎一个增强应用运行时间环境的发展，这将在 TCP/IP 网络中完全启用 UICC 应用作为安全客户端或服务器。

10.7　M2M 的安全要素的远程管理

10.7.1　综述

如上文所述，ETSI SCP 和 GlobalPlatform 规范已使用 IP 连接或无线网络载体实现了智能卡的安全远程管理功能，如 SMS 或分组交换数据载体。我们已知道，安全要素的安全远程管理要求远程管理的安全关联终点位于安全要素本身，而不是位于主机设备之中。这是与传统设备管理协议的一个重要区别，如 OMA DM 或宽带论坛 TR069。由于此区别是实现远程管理安全认证的基础，所以预计，某些用于安全要素管理和某些用于普通设备管理的这两类协议将继续共存。

然而，在当前标准下，现有 UICC 远程管理协议具有局限性，其需要在 M2M 背景下进行解决。事实上，在通信网络中假定智能卡将被彻底绑定于特定的服务订阅并由服务提供实体所拥有，而订阅变化的处理则由在终端设备（弹性漫游）中通过改变 SIM 卡来实现。如前所述，该假设不再适用于 M2M 环境，因为在 M2M 环境中，安全要素可能不再是可移动的，且一些应用需要远程管理连接而不需要物理接入设备。

10.7.2　后期个性化订阅

早期 M2M 部署出现的第一个制约条件是安全要素离开其制造工厂后订阅凭据的个性化需求。在订阅凭据嵌入主机设备后，可以将订阅凭据远程下载到安全要素中，即在已被认可的安全要素制造商工厂之外使用此方法。这就需要使用可信的并获正式许可的远程管理方案。该许可方案尤其要减少库存管理成本，通信业还有待于适应支持该项新需求的许可方案。虽然这种一次性的 OTA 订阅配置方案还未标准化，但现在已使用此方案解决服务问题，使早期的安全要素在制造过程中集成于

主机设备之中。

10.7.3 现场远程管理订阅

在这些嵌入式安全要素上，也需要以安全远程的配置方式接入凭据，并在现场发行之后，管理服务提供商之间的订阅变化，并可能在其寿命期间不止一次地进行这种方式。

10.7.3.1 现有的部署

已经出现的早期部署，如在巴西讨论的 DENATRAN（巴西政府交通运输管理局 Governmental Transport Authority）模型使用一个模块来追踪被盗汽车。在这个例子中，为 UICC 初始配置多个运营商的服务接入凭据和激活的 DENATRAN 配置文件，而管理其自己的 HLR 和 OTA 服务器的受信机构将远程负责使终端用户选择运营商的订阅。此模型为服务提供商提供了在 UICC 上管理其附加服务的功能，但其仍具有局限性，它使专有算法和凭据的预分配多达 30 个服务提供商，这就需要为终端客户提供在其服务商之间根据需要进行转换的功能。

10.7.3.2 标准化工作

为解决上述模型的局限性，并基于部署协调标准而不是专有方案，目前，ETSI SCP 正对嵌入式 UICC 的远程个性化和订阅管理方案进行标准化。这一新的努力将就以下几个方面的问题提出解决方案：

- 该方案将包括一个新功能，即管理自身的远程管理密钥并处理不同订阅的订阅管理器。订阅管理器可由生态系统中的不同参与者充当，但这些参与者必须具有阻止潜在攻击的基本功能。作为订阅管理器的参与者需要对几种模式进行区分，为适应所有可能的业务结构，在远程个性化配置以及相应的协议和文件交换格式中需要客户端和服务处理器的参与，这将可能成为标准化方案的一部分。

- 一个标准化方案向远程加载专有加密算法的实现提供了可能性，由于算法的正确书写与特定的目标硬件密切相关，需要在本机代码中写入算法，所以此算法比较难以实现。因此，应该考虑一种更具有限制性的方案，要求竞争服务提供商一致同意将共同算法（和其所有后期的演进算法）或限制性的列表预装于标准化的选择机制。

10.7.3.3 预期效益

预计引进的该嵌入式安全要素与远程管理方案对以下几个方面有益：

- 由于在个性化之前分布安全要素与设备，所以安全要素的分布成本降低。这消除了安全要素的贮存需求。
- 设备一安装就立即对订阅进行配置/个性化，安装后才具有订阅费用。
- 订阅类型可在最后时刻决定，或甚至随时间而变化，这将具有更大的灵活性。

● 对所有属于同一组的订阅做大量有效地变化（可能使用广播技术），例如，向特定类型的目标设备加载适当的安全应用。

总之，由于该嵌入式安全要素具有更大的灵活性和动态数量配置过程，所以预计其可降低订阅管理成本。

10.7.3.4　尚待解决的问题

除了标准化，该产业还需要解决远程订阅管理方案产生的一些问题，包括：

● 嵌入式安全要素拥有所有权之前、期间和之后分配新的订阅。

● 在重新分配到新服务提供商过程中发生的责任赔偿问题。

● 订阅发生变化后的安全要素的保修条款的制定方式及其内容。

参考文献

[EUSD] Directive 2002/22/EC of the European Parliament and the Council of 7 March 2002 on Universal Service and Users' Right Relating to Electronic Communications Network and Services.

[TS102221] ETSI TS 102 221. Smart Cards; UICC-Terminal Interface; Physical and Logical Characteristics (2011).

[TS102671] ETSI RTS/SCP-T090071v910 Smart Cards; Machine to Machine UICC; Physical and logical characteristics (Release 9, 2011).

[TS102241] ETSI TS 102 241. Smart Cards; UICC Application Programming Interface (UICC API) for Java Card (TM) (2011).

[TS102223] ETSI TS 102 223. Smart Cards; Card Application Toolkit (CAT) (2011).

[TS102225] ETSI TS 102 225. Smart Cards; Secured packet Structure for UICC Based Applications (2011).

[TS102226] ETSI TS 102 226. Smart Cards; Remote APDU Structure for UICC Based Applications (2011).

[TS102600] ETSI TS 102 600. Smart Cards; UICC-Terminal Interface; Characteristics of the USB Interface (2010).

[TS102613] ETSI TS 102 613. Smart Cards; UICC-CLF Interface; Physical and Data Link Layer Characteristics (2011).

[TS102622] ETSI TS 102 622. Smart Card; UICC-Contactless Front-end (CLF) Interface, Host Controller Interface (HCI) (2011).

[TS102483] ETSI TS 102 483. Smart Cards; UICC-Terminal Interface; Internet Protocol Connectivity Between the UICC and Terminal (2009).

[TS102484] ETSI TS 102 484. Smart Cards; Secure Channel Between a UICC and an End-Point Terminal (2011).

[JESD22Vib] JEDEC JESD22-B103B. (2002) Variable Frequency Vibration, http://jedec.org/download.

[JESD22Shk] JEDEC JESD22-B104C. (2004) Mechanical Shock, http://jedec.org/download.

[TS27.007] GPP TS 27.007. 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; AT command set for User Equipment (UE) (2011).

[GP22] GlobalPlatForm (2006) "GlobalPlatform Card Specification", Version 2.2 Including "Errata and Precision List" Version 0.2, http://www.globalplatform.org/.

[GP22A] GlobalPlatform (2009) GlobalPlatform Card Specification Version 2.2, Amendment A Version 1.0 Including "Errata and Precisions" Version 1.0.

[OMASCWS] OMA (2007) "Smart Card-Web-Server", OMA-TS-Smart Card-Web-Server-V1-0-20070209-C.

第 3 部分

本书结语及对未来的展望

第11章　结　　语

David Boswarthick[1]，Omar Elloumi[2]
[1]ETSI，索菲亚科技园，法国
[2]阿尔卡特朗讯，维利兹，法国

从早期 M2M 部署中学到的教训已经清楚地认定了开发一组操作习惯做法的需要，以促进 M2M 市场的所需增长。

此外，适用于所有主要 M2M 细分市场的常见功能目前正在标准化组织和全球论坛发展。这些常见的能力的发展应该逐渐降低运营部署时间表，以及使成本结构对潜在的早期采用者更加有吸引力。对市场演变来说，在最初 M2M 服务部署期间通过考虑学到的经验教训和为 M2M 系统积极促成一个标准的、可重用的框架，这是重要的。这将确保设备和服务互操作性，以及一个可以应用到全球范围内的 M2M 解决方案。

《M2M 通信：一种系统方法》，这个系列中的第一本书，使用服务需求和系统驱动方法审查了 M2M 的主题。其目的是当开发 M2M 市场确定的服务时，为读者提供一个应该被考虑的主要问题的概述。这些问题包括网络优化、服务架构、API、安全性和智能卡、M2M 设备和模块，以及 IP 协议栈演变，但这个不是详尽的列表。这些关键问题都被认为是 M2M 水平的和全球通用的功能。

然而，由于不同细分市场都有各自特定的需求，所以对所有 M2M 行业没有单一的解决方案。这使得对于大规模商业的部署，只根据这些水平的能力是几乎不可能的。尤其是在考虑到 M2M 数据模型和家里或者甚至在任何部署有传感器和 M2M 设备的建筑环境中都需要的特定连接性解决方案的时候。虽然数据模型和 M2M 局域网的多个和经常成熟的标准确实存在，但由于激烈的市场竞争和 M2M 业务的不断演变，它们一般是永久性的演变。一个市场向前发展所面临的挑战是，在标准化的单一水平结构中大量大多不兼容的传感器技术的集成。这现在成为标准化组织中的一个热门话题，如 ETSI M2M。本系列的第二本书《物联网：关键应用和协议》中提供了这个问题和类似问题的答案。

第二本书进一步介绍了 M2M，让读者熟悉了 M2M 个人垂直应用方面。这些包括智能计量、智能电网、家庭和建筑自动化，以及这些领域中涉及的具体技术，如 ZigBee 和 PLC。

在写这些书期间，作者遇到的一个主要困难是 M2M 领域内不同标准的相对不

成熟。目标在一直变化，这清楚地表明 M2M 全球标准仍在相对早期的发展阶段，也是与生俱来就与发展市场联系起来的。

例如，两个致力于 M2M 的主要标准团体：ETSI 和 3GPP。在这两个标准团体中，实际上数百个 M2M 相关的贡献在每次会议上都被提交，引入新功能，改进功能和校准。为了使这些书与读者有关，考虑到标准发展的等级，很明显，第一本书最好使用一个系统和体系结构的方法。这样一个来自许多大型 ICT 公司的高容量产业贡献和投资是清楚的证据，证明 M2M 将有影响深远，不仅在 ICT 标准生态系统和由此产生的在未来几年将被部署的系统，而且还在我们的日常生活中。M2M，未来的物联网服务和应用肯定会在这十年有深远的影响，把技术创新带进家庭和工作场所，并帮助我们的星球更“绿色”、更清洁。全球标准只是这条路的一个跳板，但它是确保顺利推出创新的 M2M 解决方案必不可少的一个。

附录　缩　略　语

3GPP	第三代合作伙伴计划
6LoWPAN	低功耗和有损网络上的 IPv6
AAA	认证、授权和计费
ABRO	权威的边界路由器选项
ADC	模-数转换器
AKA	认证和密钥协商
ALG	应用层网关
AMPS	美国移动电话服务
AODV	Ad hoc 按需距离矢量
API	应用程序编程接口
APN	接入点名称
ARO	地址注册选项
ARP	分配和保持优先级
ARPU	每用户平均收入
ARRA	美国复苏与再投资法案
ATM	自动取款机
B2B	企业对企业
B2C	企业对消费者
BGA	球栅阵列
BOM	材料清单
CA	认证机构
CAPEX	资本性支出
CAT	卡应用工具包
CBC	小区广播中心
CCF	CDMA 认证论坛
CDMA	码分多址
CDR	计费数据记录
CEN	欧洲标准化协会
CENELEC	欧洲电子技术标准化协会

CHAP	挑战认证协议
CID	连接标识符
CIDR	无类别域间路由
CM	配置管理
CoAP	约束应用协议
CRL	证书撤销列表
CSD	电路交换数据
CSP	通信服务提供商
DA	设备应用
DAD	地址冲突检测
DAO	DODAG 广告对象
DAR	发现地址请求
DHCP	动态主机配置协议
DIO	DODAG 信息对象
DIS	DODAG 信息征集
DLMS	设备语言报文规范
DM	设备管理
DNS	域名服务器
DODAG	面向对象有向非循环图
DoE	美国能源部
DPWS	web 服务器的设备配置
DSCL	设备服务功能层
DSCP	差分服务控制点
DTLS	数据报传输层安全性
DTMF	双音多频
EAB	扩展接入控制
EAL	评估保证级别
EAP	可扩展认证协议
ECC	椭圆曲线密码体制
EEPROM	电可擦可编程只读存储器
ESO	欧洲标准化组织
ETSI	欧洲电信标准化协会
EUSD	欧洲通用服务指令
EV	电动汽车
EVDO	演进数据优化

FCC	美国联邦通信委员会
FDMA	频分多址
FOTA	空中固件
FP8	第 8 个框架计划
FQDN	完全合格的域名
FTP	文件传输协议
FTTH	光纤到户
GBA	通用引导架构
GCF	全球认证论坛
GGSN	网关 GPRS 支持节点
GMSC	GSM 移动业务交换中心
GP	全局前缀
GPIO	通用输入输出
GPRS	通用分组无线业务
GPS	全球定位系统
GPSK	广义预共享密钥
GRE	通用路由封装
GSCL	网关服务功能层
GSM	全球移动通信系统
GSMA	GSM 协会
GW	网关
H2H	人对人
HCI	主机控制器接口
HLIM	跳数限制
HLR	归属位置寄存器
HSPA	高速分组接入
HSS	归属用户服务器
HTTP	超文本传输协议
IBAKE	基于身份认证的密钥交换
IBE	基于身份加密
IC	集成电路
ICCID	集成电路卡标识符
ICMP	互联网控制消息协议
ICS	车载系统
ICT	信息与通信技术

IDE	集成开发环境
IETF	互联网工程任务组
IID	接口识别
IKE	互联网密钥交换
IMEI	国际移动设备标识符
IMEISV	IMEI 软件版本
IMS	IP 多媒体子系统
IMSI	国际移动用户识别码
IoT	物联网
IOT	互操作性测试
IP	互联网协议
IPHC	IP 报头压缩
IPSEC	互联网协议安全性
ISC	IMS 服务控制
IS-IS	中间系统到中间系统
ITU	国际电信联盟
J2EE	Java 2 企业版
KGF	密钥生成功能
LAN	局域网
LBR	LoWPAN 边界路由器
LDAP	轻量级目录接入协议
LGA	线栅阵列
LLN	低功耗和有损网络
LTE	长期演进
M2M	机器对机器
M2ME	M2M 设备
MAC	媒体接入控制
MAS	M2M 认证服务器
M-BUS	仪表总线
MCM	多芯片模块
MEID	移动设备标识符
MIMO	多输入多输出
MME	移动性管理实体
MMI	人机界面
MNC	移动网络代码

MNO	移动网络运营商
MO	管理对象
MP2P	多点对点
MPLS	多协议标签交换
MRHOF	具有滞后目标函数的最低等级
MSC	移动交换中心
MSF	M2M 服务引导功能
MSIM	M2M 服务识别模块
MSIN	移动用户标识号
MSISDN	移动台国际用户目录编号
MTC	机器类通信
MTC-GW	机器类通信网关
MTU	最大传输单元
MVNO	移动虚拟网络运营商
NA	网络应用
NAPT	网络地址和端口转换
NAS	非接入层
NAT	网络地址转换
NBMA	非广播多址
NC	节点确认
NDIS	网络驱动接口规范
NDP	邻居发现协议
NFC	近场通信
NGC	网络通用通信
NGN	下一代网络
NIST	美国国家标准与技术研究院
NR	节点注册
NRPCA	网络请求的 PDP 环境激活
NS	邻居征集
NSCL	网络服务功能层
NSEC	网络安全能力
NTACS	窄带总接入通信系统
NUD	邻居不可达检测
OC	选项数
OCS	在线计费服务

OCSP	在线证书状态协议
OFDMA	正交频分多址接入
OLSR	优化的链路状态路由
OMA	开放移动联盟
OPEX	运营成本
OS	操作系统
OSPF	开放的最短路径优先
OTA	空中
OTASP	空中业务提供
P2MP	点对多点
PAK	口令认证的密钥交换
PAN	个人区域网络
PAP	密码认证协议
PCB	印制电路板
PCM	脉冲编码调制
PCRF	策略和计费规则功能
PDA	个人数字助理
PDN	分组数据网
PDP	分组数据协议
PDP-C	分组数据协议环境
PDSN	分组数据服务节点
PGW	PDN（公共数据网）网关
PIN	个人识别码
PKI	公钥基础设施
PLC	电力线通信
PM	绩效管理
PoS	销售点
PS	分组交换
PSAP	公共安全应答点
PTCRB	PCS 终端认证评估委员会
PWM	脉冲宽度调制
QoS	服务质量
RA	注册机构
RA	路由器通告
RAN	无线接入网络

RAT	无线接入技术
REST	表述性状态转移
RF	射频
RFC	征求意见
RFID	射频识别
RIP	路由信息协议
RNC	无线网络控制器
RoI	投资回报
RPL	LLN（低功耗和有损网络）的路由协议
RRC	无线资源控制
RSSI	接收信号的强度指标
SAC	源地址压缩
SAM	源地址模式
SC	服务能力
SCADA	监控与数据采集
SCP	智能卡平台
S-CSCF	服务呼叫会话控制功能
SDK	软件开发工具包
SDO	标准化开发组织
SGSN	服务 GPRS 支持节点
SGW	服务网关
SID	子网络标识符
SIM	用户识别模块
SLAAC	无状态自动地址配置
SLLAO	源链路层地址选项
SMS SC	SMS 服务中心
SMS	短消息服务
SMS-C	短消息服务中心
SMT	表面贴装技术
SMTP	简单邮件传输协议
SNMP	简单网络管理协议
SNR	序列号
SOA	面向服务的体系结构
SOAP	简单对象接入协议
TACS	总接入通信系统

TCG	可信计算组
TCO	总所有成本
TCP	传输控制协议
TDMA	时分多址
TD-SCDMA	时分同步码分多址
TIS	总的全向灵敏度
TLS	传输层安全性
TLS-PSK	传输层安全预共享密钥
TLV	类型/长度/数值
TRP	总辐射功率
TTM	上市时间
UART	通用异步接收器/发送器
UATI	单播接入终端标识符
UDC	通用十进制分类法
UDDI	通用的描述、发现和集成
UDP	用户数据报协议
UE	用户设备
UICC	通用集成电路卡
ULA	唯一本地地址
UMB	超移动宽带
UMTS	通用移动通信系统
USB	通用串行总线
USIM	通用用户识别模块
VLR	服务位置寄存器
VPN	虚拟专用网络
WAN	广域网
WLAN	无线局域网
WPAN	无线个人局域网
WSDL	web 服务描述语言
WSN	无线传感器网络
WWAN	无线广域网
xDSL	各种类型数字用户线路

读者需求调查表

个人信息

姓　　名：		出生年月：		学　　历：	
联系电话：		手　　机：		E-mail：	
工作单位：				职　　务：	
通讯地址：				邮　　编：	

1. 您感兴趣的科技类图书有哪些？

☐ 自动化技术　☐ 电工技术　☐ 电力技术　☐ 电子技术　☐ 仪器仪表　☐ 建筑电气

☐ 其他（　　）

以上各大类中您最关心的细分技术（如 PLC）是：（　　）

2. 您关注的图书类型有：

☐ 技术手册　☐ 产品手册　☐ 基础入门　☐ 产品应用　☐ 产品设计　☐ 维修维护

☐ 技能培训　☐ 技能技巧　☐ 识图读图　☐ 技术原理　☐ 实操　☐ 应用软件

☐ 其他（　　）

3. 您最喜欢的图书叙述形式：

☐ 问答型　☐ 论述型　☐ 实例型　☐ 图文对照　☐ 图表　☐ 其他（　　）

4. 您最喜欢的图书开本为：

☐ 口袋本　☐ 32 开　☐ B5　☐ 16 开　☐ 图册　☐ 其他（　　）

5. 您常用的图书信息获得渠道为：

☐ 图书征订单　☐ 图书目录　☐ 书店查询　☐ 书店广告　☐ 网络书店　☐ 专业网站

☐ 专业杂志　☐ 专业报纸　☐ 专业会议　☐ 朋友介绍　☐ 其他（　　）

6. 您常用的购书途径为：

☐ 书店　☐ 网络　☐ 出版社　☐ 单位集中采购　☐ 其他（　　）

7. 您认为图书的合理价位是（元/册）：

手册（　　）　图册（　　）　技术应用（　　）　技能培训（　　）　基础入门（　　）

其他（　　）

8. 您每年购书费用为：

☐ 100 元以下　☐ 101200 元　☐ 201300 元　☐ 300 元以上

9. 您是否有本专业的写作计划？

☐ 否　☐ 是（具体情况：　　　　）

非常感谢您对我们的支持，如果您还有什么问题欢迎和我们联系沟通！

地址：北京市西城区百万庄大街 22 号　机械工业出版社电工电子分社　邮编：100037

联系人：张俊红　联系电话：13520543780　传真：010-68326336

电子邮箱：buptzjh@ 163. com（可来信索取本表电子版）

编著图书推荐表

姓　　名：		出生年月：		职称/职务：		专　　业：	
单　　位：				E-mail：			
通讯地址：						邮政编码：	
联系电话：		研究方向及教学科目：					
个人简历（毕业院校、专业、从事过的以及正在从事的项目、发表过的论文）：							
您近期的写作计划有：							
您推荐的国外原版图书有：							
您认为目前市场上最缺乏的图书及类型有：							

地　址：北京市西城区百万庄大街 22 号　机械工业出版社　电工电子分社
邮　编：100037　　网　址：www. cmpbook. com
联系人：张俊红　　电　话：13520543780　010-68326336（传真）
E-mail：buptzjh@163. com（可来信索取本表电子版）

关于本书

本书紧跟M2M应用的最新发展，结合M2M工程应用的研究成果，采用通俗易懂的语言阐述相关技术，内容系统全面，材料充实丰富。在文字叙述中突出基本概念、基本理论及系统涉及的核心技术，同时对M2M的业务模式进行了探讨，重点讲述M2M系统的特点及相关技术的使用。本书还对M2M的架构及协议进行了详细的介绍，并对M2M技术的未来发展进行了展望。读者通过对各章节的学习，将对构建M2M应用系统有一个较为全面的认识，从中学习到M2M技术核心理论，为M2M系统的实施及应用打下良好的基础。

为中华崛起传播智慧

地址：北京市百万庄大街22号
邮政编码：100037

电话服务
社服务中心：010-88361066
销售一部：010-68326294
销售二部：010-88379649
读者购书热线：010-88379203
网络服务
教材网：http://www.cmpedu.com
机工官网：http://www.cmpbook.com
机工官博：http://weibo.com/cmp1952

封面无防伪标均为盗版

策划编辑◎牛新国

国际视野　科技前沿

国际信息工程先进技术译丛

《M2M通信》
《面向IMT-Advanced及Beyond的移动无线通信》
《成功的电信服务设计——设计与实现的全面指南》
《IP地址管理原理与实践》
《自组织网络：GSM，UMTS和LTS的自规划、自优化和自愈合》
《UMTS中的LTE：向LTE-Advanced演进》（原书第2版）
《UMTS中的WCDMA-HSPA演进及LTE》（原书第5版）
《LTE自组织网络（SON）：网络管理自动化提升运维效率》
《实现吉比特传输的60GHz无线通信技术》
《内容分发网络》
《无线Mesh网络架构与协议》
《UMTS蜂窝系统的QoS与QoE管理》
《半导体制造与过程控制基础》
《下一代移动系统：3G/B3G》
《IMS:IP多媒体概念和服务》（原书第2版）
《下一代无线系统与网络》
《深入浅出UMTS无线网络建模、规划与自动优化：理论与实践》
《HSDPA/HSUPA技术与系统设计——第三代移动通信系统宽带无线接入》
《无线传感器及元器件：网络、设计与应用》
《印制电路板——设计、制造、装配与测试》
《IPTV与网络视频：拓展广播电视的应用范围》
《多电压CMOS电路设计》
《微电子技术原理、设计与应用》
《蜂窝网络高级规划与优化2G/2.5G/3G/…向4G的演进》
《基于蜂窝系统的IMS——融合电信领域的VoIP演进》
《无线网络中的合作原理与应用》
《环境网络：支持下一代无线业务的多域协同网络》
《基于射频工程的UMTS空中接口设计与网络运行》
《未来UMTS的体系结构与业务平台：全IP的3G CDMA网络》
《UMTS-HSDPA系统的TCP性能》
《宽带无线通信中的空时编码》
《数字图像处理》（原书第4版）
《基于4G系统的移动服务技术》
《吉规模集成电路互连工艺及设计》
《高性能微处理器电路设计》

WILEY

Copies of this book sold without a Wiley Sticker on the cover are unauthorized and illegal



上架指导　工业技术／通信技术

ISBN 978-7-111-41693-7　定价：68.00元